Wi² AP CLI

Reference Guide

SW Version 5.2
June 2008
P/N 215031

Legal Rights

© Copyright 2008 Alvarion Ltd. All rights reserved.

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMANAGE™, BreezeLINK®, BreezeConfig™, BreezeMAX™, AlvariSTAR™, AlvariCRAFT™, BreezeLITE™, MGW™, eMGW™, and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from

invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER

WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Disposal of Electronic and Electrical Waste

Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

About This Guide

This guide describes the Wi² AP CLI.

This guide comprises the following parts:

- Chapter 1 - “Introduction” on page 1
- Chapter 2 - “CLI Commands” on page 11

Contents

Chapter 1 - Introduction

1.1 About this guide 2

1.1.1 Products covered 2

1.1.2 Important terms 2

1.1.3 Typographical conventions 2

1.2 CLI support in autonomous and controlled modes 4

1.2.1 Controlled mode 4

1.2.2 Autonomous mode 4

1.3 Configuring CLI support 5

1.4 SSH client support 7

1.5 Entering strings 8

1.6 Context Hierarchy 9

Chapter 2 - CLI Commands

2.1 View Context 12

arping 12
curl 12
enable 14
nslookup 15
ping 15
ps 15
quit 15
show license 15
show logging filtered 15
top 15
traceroute 16

2.2 Enable Context 17

reboot device 17
show certificate 17
show certificate binding 17
ping 17
arping 17

arp 18
end 18
quit 18
rcapture 18
show arp 18
show bridge 18
show bridge forwarding 18
show dns cache 19
show interfaces 19
show ip route 19
show system info 19
factory reset 19
switch operational mode 19
show dot11 associations 19
show dot11 statistics client-traffic 20
show local mesh 20
show wireless neighborhood 20
show wireless rogue-ap 20
show client log 20
config 20
show all config 20

2.3 Config Context 21

certificate 21
certificate binding 21
certificate revocation 21
end 21
factory settings 21
interface ethernet 21
reboot device 22
show certificate 22
show certificate binding 22
show config 22
username 22
interface ip 22
interface wireless 22
local mesh profile 23
interface gre 23
virtual ap 23
admin authentication local fallback 23
admin authentication radius 23
clock summer-time 24
clock timezone 24
ip http port 24
ip https port 24
ntp protocol 25
ntp server 25
snmp-server trap certificate-expired 25
snmp-server trap certificate-expires-soon 25
snmp-server trap web-fail 25
snmp-server trap web-login 26
snmp-server trap web-logout 26

web admin kickout 26
web allow 26
world-mode dot11 country code 26
web access port-1 27
web access port-2 27
web access wireless 27
web access interface vlan 27
web access interface gre 27
web access local mesh 28
clock 28
ntp server 28
ntp server failure trap 28
config-update automatic 28
config-update operation 29
config-update time 29
config-update uri 29
config-update weekday 29
snmp-server trap config-change 29
snmp-server trap config-update 30
logging destination 30
snmp-server trap syslog-severity 30
snmp-server 30
snmp-server access port-1 30
snmp-server allow 31
snmp-server chassis-id 31
snmp-server contact 31
snmp-server heartbeat period 31
snmp-server location 32
snmp-server port 32
snmp-server readonly 32
snmp-server readwrite 32
snmp-server trap 32
snmp-server trap community 33
snmp-server trap destination 33
snmp-server trap heartbeat 33
snmp-server trap link-state 33
snmp-server trap snmp-authentication 33
snmp-server version 34
snmp-server access interface vlan 34
snmp-server access local mesh 34
snmp-server access interface gre 34
snmp-server access wireless 34
snmp-server access port-2 34
soap-server 35
soap-server access interface vlan 35
soap-server access port-1 35
soap-server access port-2 35
soap-server allow 35
soap-server http authentication 36
soap-server http authentication password 36
soap-server http authentication username 36
soap-server port 36

soap-server ssl 36
soap-server ssl with client certificate 36
soap-server access interface gre 37
soap-server access wireless 37
soap-server access local mesh 37
snmp-server trap low-snr 37
snmp-server trap low-snr interval 37
snmp-server trap low-snr level 38
snmp-server trap new-association 38
snmp-server trap new-association interval 38
snmp-server trap vpn-connection 38
snmp-server trap wireless-association-fail 38
snmp-server trap wireless-association-success 38
snmp-server trap wireless-authentication-fail 39
snmp-server trap wireless-authentication-success 39
snmp-server trap wireless-deauthentication-fail 39
snmp-server trap wireless-deauthentication-success 39
snmp-server trap wireless-disassociation-fail 39
snmp-server trap wireless-disassociation-success 40
snmp-server trap wireless-reassociation-fail 40
snmp-server trap wireless-reassociation-success 40
snmp-server trap syslog-matches 40
snmp-server trap syslog-matches regex 40
snmp-server trap syslog-severity level 40
snmp-server trap network-trace 41
firmware-update automatic 41
firmware-update start 41
firmware-update time 41
firmware-update uri 42
firmware-update weekday 42
snmp-server trap firmware-update 42
access-controller restrict location 42
service-sensor 42
service-sensor 43
service-sensor poll 43
service-sensor retry 43
service-sensor timeout 43
ip name-server 44
ip name-server cache 44
ip name-server dynamic 44
ip name-server switch-on-servfail 44
ip name-server switch-over 45
snmp-server trap unauthorized-ap 45
snmp-server trap unauthorized-ap interval 45
wireless-scan 45
wireless-scan period 45
wireless-scan url 45
access controller shared secret 46
radius-server profile 46
ip-qos profile 46
dot11 igmp snooping-helper 47
discovery protocol 47

discovery protocol device-id 47
bridge priority 47
bridge protocol ieee 48
bridge protocol ieee vlan 48
ip route gateway 48
dot1x reauth 48
dot1x reauth period 49
dot1x reauth terminate 49
dot1x supplicant timeout 49
dynamic key 49
dynamic key interval 49
add wireless ip-qos profile 50
delete wireless ip-qos profile all 50
delete wireless ip-qos profile 50
wireless link qos 50
sensor discovery mode 50
sensor network detector 51
sensor server id 51
sensor server name 51
config-version 51

2.4 Port-2 Interface Context 52

duplex 52
end 52
speed 52
vlan 52
vlan compatibility mode 53
vlan-management filter 53
interface vlan 53

2.5 Port-1 Interface Context 54

duplex 54
end 54
speed 54
vlan 54
vlan compatibility mode 55
vlan-management filter 55
interface vlan 55

2.6 WAN IP Interface Context 56

pppoe client user 56
ip address mode 56
ip address 56
ip address dhcp client-id 57
end 57
pppoe auto-reconnect 57
pppoe mru 57
pppoe mtu 57
pppoe unnumbered 58

2.7 Wireless Context 59

end 59

radio active 59
rts threshold 59
distance 60
dot11 60
transmit power 60
antenna bidirectionnal 61
autochannel skip 61
beacon interval 61
dot11 automatic frequency 61
dot11 automatic frequency period 62
dot11 automatic frequency time 62
dot11 automatic transmit-power 62
dot11 automatic transmit-power period 62
multicast rate 62
station distance 63
dot11 mode 63
bandwidth 63
bandwidth max 63

2.8 Virtual AP Context 64

virtual ap name 64
access controller 64
ingress interface 64
max-association 65
ssid name 65
vlan 65
guest-mode 65
encryption key 1 65
encryption key format 66
transmit key 66
authentication server access controller 66
authentication server accounting 66
authentication server accounting radius profile 67
authentication server radius 67
wpa-psk 67
authentication server accounting radius stationid case 67
authentication server accounting radius stationid delimiter 67
wireless filters 68
wireless filters mac 68
wireless filters rule input 68
wireless filters rule output 68
wireless filters type 69
mac-filters local 70
mac-filters 70
mac-filters mode 71
mac authentication accounting 71
mac authentication accounting radius profile 71
mandatory authentication 71
mac authentication radius profile 71
mac authentication radius stationid case 71
mac authentication radius stationid delimiter 72
mac authentication 72

dot1x mandatory authentication 72
add ip filter 72
delete ip filter 72
delete ip filter all 73
ip filters 73
active 73
beacon dtim count 73
public forwarding 73
fast authentication 74
layer3 mobility 74
beacon transmit power 74
data rate maximum 74
data rate minimum 74
add ip-qos profile 75
delete ip-qos profile all 75
delete ip-qos profile 75
qos 75
upstream diffserv tagging 76
wmm advertising 76
location-aware group 77
end 77
security 77

2.9 VLAN interface Context 78

end 78
ip address 78
ip address mode 78
vlan name 79

2.10Local Mesh Context 80

end 80
active 80
interface 80
local mesh name 80
remote mac 80
security 81
security mode 81
security psk 81
security wep 81
speed 81
interface vlan 81
accept forced links 82
allowed downtime 82
dynamic local mesh 82
dynamic mode 82
initial discovery time 82
mesh id 82
minimum snr 83
preserve master link 83
promiscuous mode 83
promiscuous mode startup delay 83

snr cost per hop 83
2.11RADIUS Context 84
end 84
radius-server accounting port 84
radius-server alternate hosts 84
radius-server authentication method 84
radius-server authentication port 85
radius-server deadtime 85
radius-server host 85
radius-server key 2 85
radius-server message-authenticator 85
radius-server name 86
radius-server nasid 86
radius-server timeout 86
radius-server timeout 86
2.12IP_QOS Context 87
end 87
end-port 87
priority 87
profile name 87
protocol 87
start-port 88
2.13GRE Interface Context 89
end force 89
gre name 89
ip address 89
peer ip address 89
remote ip address 89
2.14Syslog Destination Context 90
active 90
logging facility 90
logging host 90
logging prefix 90
name 90
end 91
level 91
level 91
matches 91
message 91
message 92
process 92
process 92

1

Chapter 1 - Introduction

In This Chapter:

- "About this guide" on page 2
- "CLI support in autonomous and controlled modes" on page 4
- "Configuring CLI support" on page 5
- "SSH client support" on page 7
- "Entering strings" on page 8
- "Context Hierarchy" on page 9

1.1 About this guide

This guide explains how to work with the Command Line Interface (CLI) on Alvarion MultiService Access Points points operating in autonomous mode.

1.1.1 Products covered

This guide covers these access points:

- Wi^2 AP

1.1.2 Important terms

The following terms are used in this guide.

Term	Description
AP, MAP	These terms are used interchangeably to to refer to any Alvarion MultiService Access Point as defined in *Products Covered* above.
service controller, MSC	These terms are used interchangeably to refer to any Alvarion MultiService Controller.
Wi^2 AP	These product name references also include the R versions .
local mesh	Previously referred to as WDS. Some older commands refer to “wireless links” whereas newer commands use the “local mesh” terminology and they also provide dynamic functionality.
Virtual MAPmap, VAP	In this document, the terms “Virtual MAPmap” and “VAP” are used in place of “VSC” (Virtual Service Community).

1.1.3 Typographical conventions

1.1.3.1 Command syntax

Command syntax is formatted in a monospaced font as follows:

Example	Description
`use-access-list`	Command name. Specify it as shown.

Example	Description
`ip-qos profile <name>`	A single item enclosed in angle brackets and all formatted in italic indicates a user-supplied item. Specify the item. Do not include the angle brackets. In this example, a valid QoS profile name is required. For example: `ip-qos profile voice`
`wireless interface (1|2)`	Multiple Items enclosed in parenthesis and separated by vertical bars indicate a mandatory choice. Include one of the mandatory items, without the parenthesis and without the vertical bar. In this example, either 1 or 2 must be included. For example: `wireless interface 2`

`show logging [filtered]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can specify the command in one of two ways:
	`show logging`
	`show logging filtered`

1.1.3.2 Management tool

When referring to the management tool interface, the Main menu name is presented first followed by a right angle-bracket and then the sub-menu name, as in **Network > Ports**.

1.2 CLI support in autonomous and controlled modes

An AP operates in either controlled mode or autonomous mode.

1.2.1 Controlled mode

Controlled mode is the factory default mode for all APs.

When in controlled mode, an AP establishes a control channel with a Wi2 Controller series service controller. The service controller manages the AP and provides all configuration settings. Discovery of the service controller is automatic if default settings are used on all devices.

NOTE

In controlled mode, access to the CLI is possible only before any control channel is established, which can occur in the following scenarios:

- Network failures prevent a control channel from being created.
- After a AP is restarted, prior to establishment of the control channel (during the brief service controller discovery process).

When the AP is in controlled mode, a reduced number of CLI commands are available. The most notable command is **switch operational mode**, which enables you to switch the AP to autonomous mode. Also, the config context is not available.

1.2.2 Autonomous mode

When in autonomous mode, the AP operates as a stand-alone unit. You can configure and manage the AP using the AP's management tool, SNMP, CLI, or SOAP. Autonomous mode supports all CLI commands.

1.3 Configuring CLI support

Using the AP's management tool, open the page **Management > CLI**. Use this page to enable/disable CLI support via an SSH or serial connection. A maximum of three concurrent CLI sessions are supported regardless of the connection type.

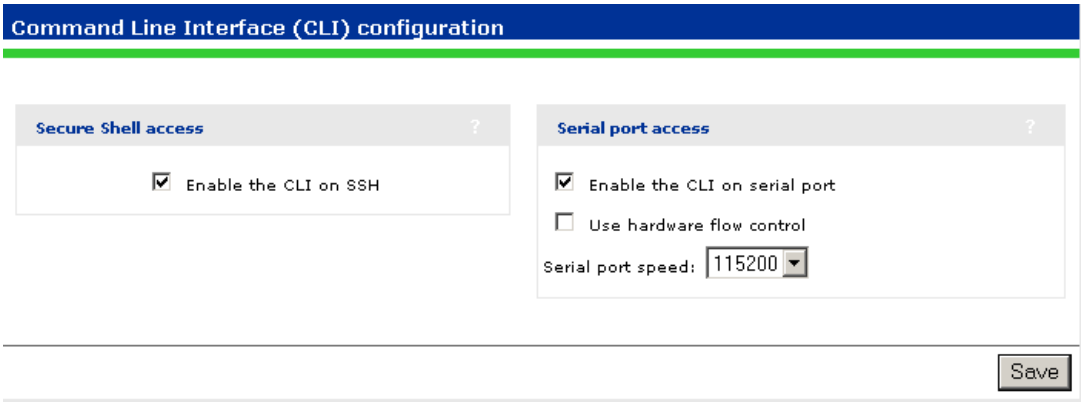

Figure 1-1: Command Line Interface (CLI) Configuration

The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for management tool administrators on the **Management > Management tool** page.

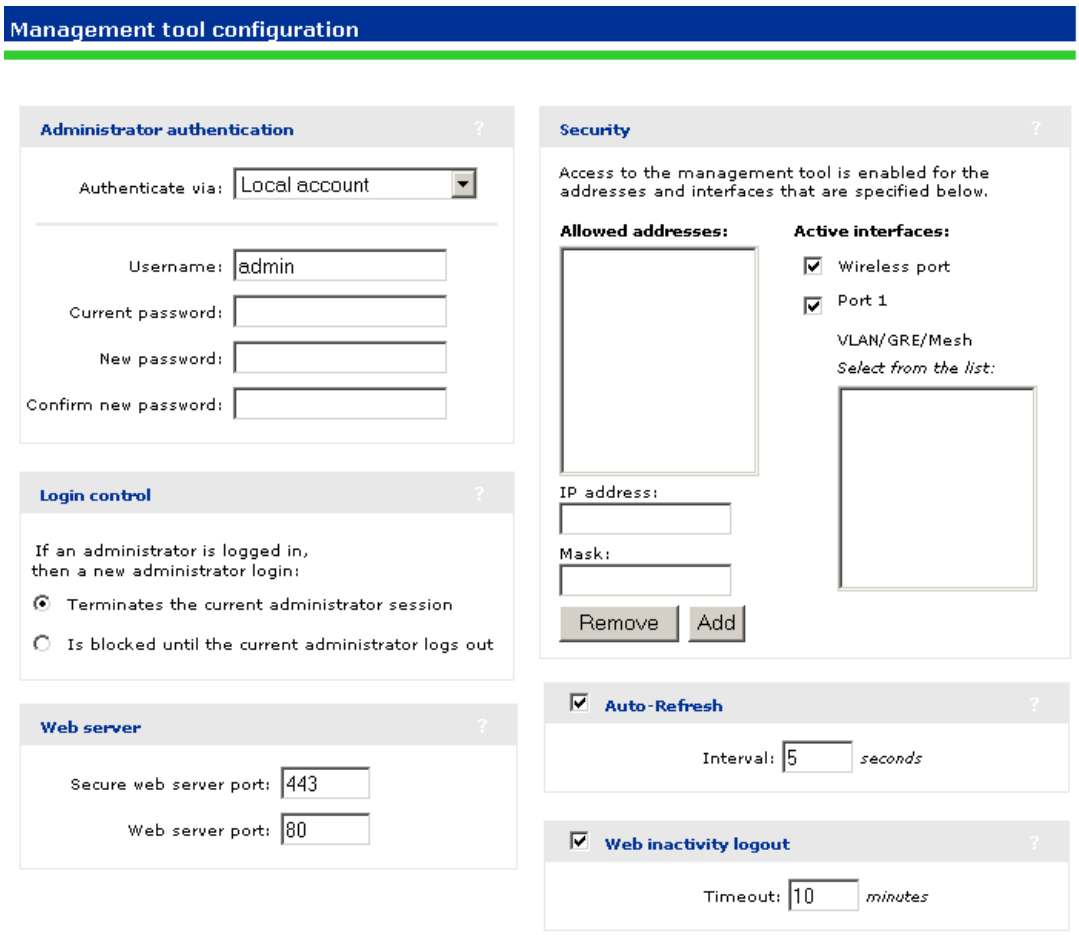

Figure 1-2: Management Tool Configuration

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security.**

- The login credentials for SSH connections are the same as those defined under **Administrator authentication**. By default, both username and password are set to **admin**.

NOTE

SSH logins always use the local administrator username and password, even if **Administrator authentication** is set to use an external RADIUS server.

1.4 SSH client support

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty

1.5 Entering strings

When entering a value that contains spaces, you must enclose it in quotation marks. For example, if the command syntax is:

```
ssid <name>
```

you must specify one of the following:

```
ssid ANameWithNoSpaces
ssid “A name with spaces”
```

1.6 Context Hierarchy

CLI commands are grouped into functional contexts. The following table shows the context hierarchy and the command used to switch from the parent context.

Context hierarchy	Command to switch from parent context
View context	(This is the first context.)
Enable context	enable
Config context	config
WAN IP interface context	interface ip
Internet interface context	interface ethernet *port-2*
VLAN interface context	interface vlan <*id*>[-<*id2*>]
LAN interface context	interface ethernet port-1
VLAN interface context	interface vlan <*id*>[-<*id2*>]
Wireless context	interface wireless <*number*>
Local mesh context	local mesh profile <*name*>
VLAN interface context	interface vlan <*number*>
GRE interface context	interface gre <*name*>
Virtual AP context	virtual ap <*name*>
Syslog destination context	logging destination <*name*>
RADIUS context	radius-server profile <*name*>
IP_QOS context	ip-qos profile <*name*>

2

Chapter 2 - CLI Commands

2.1 View Context

Context path: View

This is the root of the command tree.

---

arping

Supported on: Wi² AP

`arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface> <destination>`

Pings a destination on a device interface using ARP packets.

---

curl

Supported on: Wi² AP

`curl [parameter] <url>`

Use the curl command to get/send files to/from the Wi² AP.

Parameters

`-a`	**Specifies append to target file when uploading. FTP only.**
`-A <string>`	**Specifies the User-Agent to send to server. HTTP only.**
`-b <name=string>`	**Specifies the cookie string or file to read cookies from. HTTP only.**
`-B`	**Specifies to use ASCII/text transfer.**
`-c <file>`	**Specifies to write all cookies to this file after operation. HTTP only.**
`-C <offset>`	**Specifies the absolute resume offset.**
`-d data <data>`	**Specifies HTTP POST data. HTTP only.**
`--data-ascii <data>`	**Specifies HTTP POST ASCII data. HTTP only.**
`--data-binary <data>`	**Specifies HTTP POST binary data. HTTP only.**
`--data-epsv <data>`	**Prevents curl from using EPSV. FTP only.**
`-D <file>`	**Specifies to write the headers to this file.**
`--egd-file <file>`	**Specifies EGD socket path for random data. SSL only.**
`-E <cert[:passwd]>`	**Specifies a certificate file and password. HTTPS only.**
`--cert-type <type>`	**Specifies the certificate file type. HTTPS only.**
`--key <key>`	**Specifies the private key file. HTTPS only.**
`--key-type <type>`	**Specifies the private key file type. HTTPS only.**
`--pass <pass>`	**Specifies the passphrase for the private key. HTTPS only.**
`--engine <eng>`	**Specifies the crypto engine to use. HTTPS only.**
`--cacert <file>`	**Specifies the CA certificate to verify peer against. SSL only.**
`--capath <dir>`	**Specifies the CA directory to verify peer against. SSL only.**

`--ciphers <list>`	**Specifies the SSL ciphers to use. SSL only.**
`--compressed`	**Specifies to request a compressed response (using deflate).**
`--compressed`	**Specifies to request a compressed response (using deflate).**
`--connect-timeout <sec>`	**Specifies the maximum time allowed for connection.**
`--create-dirs`	**Specifies to create the necessary local directory hierarchy.**
`--crlf`	**Specifies to convert LF to CRLF in upload.**
`-f`	**Specifies to fail silently (no output at all) on errors. HTTP only.**
`-F <name=content>`	**Specifies HTTP POST data. HTTP only.**
`-g`	**Specifies to disable URL sequences and ranges using {} and [].**
`-G <name=content>`	**Specifies to send the -d data with a HTTP GET. HTTP only.**
`-h`	**Displays this help text.**
`-H <line>`	**Specifies the custom header to pass to the server. HTTP only.**
`-i`	**Specifies to include the HTTP-header in the output. HTTP only.**
`-I`	**Specifies to fetch document info only.**
`-j <cert[:passwd]>`	**Specifies to ignore session cookies read from file. HTTP only.**
`--interface <interface>`	**Specifies the interface to use.**
`--krb4 <level>`	**Specifies to enable krb4 with specified security level. FTP only.**
`-k`	**Specifies to disallow curl to connect to SSL sites without certificates. HTTP only.**
`-K`	**Specifies which config file to read.**
`-l`	**Specifies to list only names of an FTP directory FTP only.**
`--limit-rate <rate>`	**Specifies the speed limit for transfers.**
`-L`	**Specifies Follow Location: hints. HTTP only.**
`-m <seconds>`	**Specifies the maximum time allowed for the transfer.**
`-M`	**Specifies to display huge help text.**
`-n`	**Specifies to read .netrc for user name and password**
`--netrc-optional`	**Specifies to use either .netrc or URL; overrides -n**
`-N`	**Optional parameter that disables the buffering of the output stream**
`-o <file>`	**Specifies to write output to <file> instead of stdout.**
`-O`	**Specifies to write output to a file named as the remote file.**
`-p`	**Specifies to perform non-HTTP services through a HTTP proxy.**
`-P <address>`	**Specifies to use PORT with address instead of PASV when ftping. FTP only.**

`-q`	**When used as the first parameter disables .curlrc**
`-Q <cmd>`	**Specifies to send QUOTE command to FTP before file transfer. FTP only.**
`-r <range>`	**Specifies to retrieve a byte range from a HTTP/1.1 or FTP server.**
`-R`	**Sets the remote file's time on the local output.**
`-s`	**Specifies silent mode. Don't output anything.**
`-S`	**Specifies show error. With -s, make curl show errors when they occur.**
`--stderr <file>`	**Specifies where to redirect stderr. - means stdout.**
`-t <OPT=val>`	**Sets the telnet option.**
`--trace <file>`	**Dumps a network/debug trace to the given file.**
`--trace-ascii <file>`	**Specifies --trace but without the hex output.**
`-T <file>`	**Specifies to transfer/upload <file> to remote site.**
`--url <URL>`	**Specifies another way to specify URL to work with.**
`-ur <user[:pass]>`	**Specifies user and password to use. Overrides -n and --netrc-optional**
`-U <user[:pass]>`	**Specifies proxy authentication.**
`-v`	**Makes the operation more talkative.**
`-V`	**Outputs version number then quits.**
`-w [format]`	**Specifies what to output after completion.**
`-x <host[:port]>`	**Specifies to use proxy. (Default port is 1080).**
`--random-file <file>`	**Specifies the file to use for reading random data from (SSL).**
`-X <command>`	**Specifies the request command to use.**
`-y`	**Specifies the time needed to trig speed-limit abort. Defaults to 30.**
`-Y`	**Specifies to stop transfer if below speed-limit for 'speed-time' secs.**
`-z <time>`	**Includes a time condition to the server. HTTP only.**
`-Z <num>`	**Sets the maximum number of redirections allowed. HTTP only.**
`-0`	**Forces usage of HTTP 1.0. HTTP only.**
`-1`	**Forces usage of TLSv1. HTTP only.**
`-2`	**Forces usage of SSLv2. HTTP only.**
`-3`	**Forces usage of SSLv3. HTTP only.**

enable

Supported on: Wi² AP

`enable`

Switches to the enable context.

nslookup

Supported on: Wi² AP

`nslookup [ -option authentication ] [ <host-to-find> | - [< server> ]]`

Queries DNS servers for information on hosts or domains.

ping

Supported on: Wi² AP

`ping <host> [-c <count>] [-s <length>] [-q]`

Determines if the specified remote IP address is active.

Parameters

<-c host>	**The IP address or DNS name of the host to ping.**
<-c count>	**Number of pings.**
<-s length>	**Length of the ping datagram.**
<-q>	**Quiet mode. No output.**

ps

Supported on: Wi² AP

`ps`

Displays all running processes.

quit

Supported on: Wi² AP

`quit`

Quits the CLI.

show license

Supported on: Wi² AP

`show license (EULA | gpl | other)`

Displays license information.

show logging filtered

Supported on: Wi² AP

`show logging [filtered]`

Displays the system log.

top

Supported on: Wi² AP

`top`

Displays all running processes.

Press “q” to exit “top”.

traceroute

Supported on: Wi² AP

`traceroute [-n] [-r] [-v] [-m <max_ttl>] [-p <port#>] [-q <nqueries>] [-s <src_addr>] [-t <tos>] [-w <wait>] <host> [<data size>]`

Show the hosts that are traversed to reach the specified IP address.

2.2 Enable Context

Context path: View > Enable

This context provides access to various utilities.

reboot device

Supported on: Wi² AP

`reboot device`

Restarts the system.

show certificate

Supported on: Wi² AP

`show certificate`

Display current certificates.

show certificate binding

Supported on: Wi² AP

`show certificate binding`

Display how the certificates are used.

ping

Supported on: Wi² AP

`ping <host> [-c <count>] [-s <length>] [-q]`

Determines if the specified remote IP address is active.

Parameters

<-c host>	**The IP address or DNS name of the host to ping.**
<-c count>	**Number of pings.**
<-s length>	**Length of the ping datagram.**
<-q>	**Quiet mode. No output.**

arping

Supported on: Wi² AP

`arping [ -AbDfhqUV] [ -c <count>] [ -w <deadline>] [ -s <source>] -I <interface> <destination>`

Pings a destination on a device interface using ARP packets.

arp

Supported on: Wi² AP

```
arp [-evn] [-H <type>] [-i if] ?- [<hostname>] arp [-v] [-i if] -d
<hostname> [pub] arp [-v] [-H <type>] [-i if] -s <hostname>
<hw_addr> [temp] arp [-v] [-H <type>] [-i if] -s <hostname>
<hw_addr> [<netmask> <nm>] <pub> arp [-v] [-H <type>] [-i if] -Ds
<hostname> ifa [<netmask> <nm>] <pub>
```

Displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

end

Supported on: Wi² AP

```
end
```

Switches to parent context.

quit

Supported on: Wi² AP

```
quit
```

Exit the enable context.

rcapture

Supported on: Wi² AP

```
rcapture [<a>] [<b>] [<c>] [<d>] [<e>] [<f>] [<g>] [<h>]
```

Sends port capture to an FTP server.

Refer to Linux documentation for a complete description of this command and its options.

show arp

Supported on: Wi² AP

```
show arp
```

Show the ARP table.

show bridge

Supported on: Wi² AP

```
show bridge
```

Show bridge information.

show bridge forwarding

Supported on: Wi² AP

```
show bridge forwarding
```

Show bridge forwarding information.

show dns cache

Supported on: Wi² AP

`show dns cache [<serial>]`

Show DNS cache entries. Specify a serial number to display detailed information.

show interfaces

Supported on: Wi² AP

`show interfaces`

Show networking interfaces.

show ip route

Supported on: Wi² AP

`show ip route`

Show all IP routes.

show system info

Supported on: Wi² AP

`show system info`

Show basic system information.

factory reset

Supported on: Wi² AP

`factory reset`

Resets the unit to factory default settings.

switch operational mode

Supported on: Wi² AP

`switch operational mode`

Switches the unit's operational mode.

show dot11 associations

Supported on: Wi² AP

`show dot11 associations`

Show all current wireless associations.

show dot11 statistics client-traffic

Supported on: Wi² AP

`show dot11 statistics client-traffic`

Show current client matrix statistics.

show local mesh

Supported on: Wi² AP

`show local mesh`

Show current local mesh interfaces.

show wireless neighborhood

Supported on: Wi² AP

`show wireless neighborhood`

Show all access points detected nearby.

show wireless rogue-ap

Supported on: Wi² AP

`show wireless rogue-ap`

Show all rogue access points detected nearby.

show client log

Supported on: Wi² AP

`show client log [<macaddr>]`

Display client station log. Enter the MAC address to display more details for a specific client station.

config

Supported on: Wi² AP

`config`

Switches to the config context.

show all config

Supported on: Wi² AP

`show all config`

Print all configuration that applies to this device. This is equivalent to: `config > show config`.

2.3 Config Context

Context path: View > Enable > Config

This is the root context for all configuration commands.

---

certificate

Supported on: Wi² AP

`certificate (authority | local) <uri> <certname> [<password>]`

Add a new certificate to the store, using the friendly name.

---

certificate binding

Supported on: Wi² AP

`certificate binding (web-management | html-auth | soap | eap) <certname>`

Assign a certificate to a service.

`no certificate binding (web-management | html-auth | soap | eap) <certname>`

Unassign a certificate from a service.

---

certificate revocation

Supported on: Wi² AP

`certificate revocation <uri> <certname>`

Add a Certificate Revocation List to an existing authority certificate.

---

end

Supported on: Wi² AP

`end`

Switches to parent context.

---

factory settings

Supported on: Wi² AP

`factory settings`

Resets the system configuration to factory default settings.

---

interface ethernet

Supported on: Wi² AP

`interface ethernet (port-1|port-2)`

Switches to the specified Ethernet interface context.

reboot device

Supported on: Wi² AP

`reboot device`

Restarts the system.

show certificate

Supported on: Wi² AP

`show certificate`

Display current certificates.

show certificate binding

Supported on: Wi² AP

`show certificate binding`

Display how the certificates are used.

show config

Supported on: Wi² AP

`show config [factory]`

Generates a list of CLI commands that can be used to define the currently loaded configuration.

username

Supported on: Wi² AP

`username <user> <password>`

Changes the current administrator username and password.

Parameters

<user>	**New administrator username.**
<password>	**New administrator password.**

interface ip

Supported on: Wi² AP

`interface ip`

Switches to the specified IP interface context.

interface wireless

Supported on: Wi² AP

`interface wireless <interface number>`

Switches to the specified wireless interface context.

local mesh profile

Supported on: Wi² AP

`local mesh profile <name>`

Switches to the specified local mesh link context.

Parameters

<name>	**Number of the local mesh link to configure.**

interface gre

Supported on: Wi² AP

`interface gre <name>`

Switches to the specified GRE interface or creates a new GRE interface with the specified name.

`no interface gre <name>`

Deletes the specified GRE interface.

virtual ap

Supported on: Wi² AP

`virtual ap <name>`

Creates a new VAP (virtual network) profile or switches to the existing VAP (virtual network) context with the specified name.

`no virtual ap <name>`

Deletes the specified Virtual AP profile.

Parameters

name	**Name of an existing or new VAP (vertual network) profile.**

admin authentication local fallback

Supported on: Wi² AP

`admin authentication local fallback`

Allow administrators to login via the local account if the RADIUS server is unreachable.

`no admin authentication local fallback`

Do not allow administrators to login via the local account if the RADIUS server is unreachable.

admin authentication radius

Supported on: Wi² AP

`admin authentication radius <name>`

Sets the RADIUS profile to use for authentication of administrator logins.

`no admin authentication radius`

Sets the authentication of administrator logins to occur using the specified RADIUS profile.

Parameters

<name>	**RADIUS profile name.**

clock summer-time

Supported on: Wi² AP

`clock summer-time`

Enables support for daylight savings time.

`no clock summer-time`

Disables support for daylight savings time.

clock timezone

Supported on: Wi² AP

`clock timezone <gmtdiff>`

Sets the time zone the Wi² AP is operating in.

Parameters

<gmtdiff>	**Offset from GMT as follows: +-HOUR:MIN. For example, Eastern Standard time is -5:00.**

ip http port

Supported on: Wi² AP

`ip http port <number>`

Sets the port number to use for HTTP access to the Wi² AP.

Parameters

<number>	**Port number. Range: 1 - 65535.**

Description

HTTP connections made to this port are met with a warning and the browser is redirected to the secure web server port. By default. this parameter is set to port 80.

ip https port

Supported on: Wi² AP

`ip https port <number>`

Sets the port number used for HTTPS access to the Wi² AP.

Parameters

<number>	**Port number. Range: 1 - 65535.**

ntp protocol

Supported on: Wi² AP

```
ntp protocol (ntp | sntp)
```

Sets the network time protocol to use.

ntp server

Supported on: Wi² AP

```
ntp server
```

Enable this option to have the Wi² AP periodically contact a network time server to update its internal clock.

```
no ntp server
```

Disables the use of a network time server.

snmp-server trap certificate-expired

Supported on: Wi² AP

```
snmp-server trap certificate-expired
```

Send a trap when the SSL certificate has expired. A trap is sent every 12 hours.

```
no snmp-server trap certificate-expired
```

Do not send a trap when the SSL certificate has expired.

snmp-server trap certificate-expires-soon

Supported on: Wi² AP

```
snmp-server trap certificate-expires-soon
```

Send a trap when the SSL certificate is about to expire. A trap is sent every 12 hours starting 15 days before the certificate expires.

```
no snmp-server trap certificate-expires-soon
```

Do not send a trap when the SSL certificate is about to expire.

snmp-server trap web-fail

Supported on: Wi² AP

```
snmp-server trap web-fail
```

Send a trap each time an administrator login is refused.

```
no snmp-server trap web-fail
```

Do not send a trap each time an administrator login is refused.

snmp-server trap web-login

Supported on: Wi² AP

`snmp-server trap web-login`

Send a trap each time an administrator login is accepted.

`no snmp-server trap web-login`

Do not send a trap each time an administrator login is accepted.

snmp-server trap web-logout

Supported on: Wi² AP

`snmp-server trap web-logout`

Send a trap each time an administrator logs out.

`no snmp-server trap web-logout`

Do not send a trap each time an administrator logs out.

web admin kickout

Supported on: Wi² AP

`web admin kickout`

Enables a new administrator login to terminate an existing administrator session.

`no web admin kickout`

Stops a new administrator from logging in until an existing administrator logs out.

web allow

Supported on: Wi² AP

`web allow <ip address>/<mask>`

Adds an address to the list of hosts that can access the management tool.

`no web allow <ip address>/<mask>`

Removes the specified address from the list of hosts that can access the management tool.

Parameters

<address>	**IP address.**
</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

world-mode dot11 country code

Supported on: Wi² AP

`world-mode dot11 country code <code>`

Specifies the country the Wi² AP is operating in.

Parameters

<code>	**An ISO3166 three-letter country code.**

web access port-1

Supported on: Wi² AP

`web access port-1`

Enables access to the management tool via Port-2.

`no web access port-1`

Blocks access to the management tool via Port-2.

web access port-2

Supported on: Wi² AP

`web access port-2`

Enables access to the management tool via Port-1.

`no web access port-2`

Blocks access to the management tool via Port-1.

web access wireless

Supported on: Wi² AP

`web access wireless`

Enables access to the management tool via the wireless port.

`no web access wireless`

Blocks access to the management tool via the wireless port.

web access interface vlan

Supported on: Wi² AP

`web access interface vlan <name>`

Enables access to the management tool via the specified VLAN.

`no web access interface vlan <name>`

Removes access to the management tool for the specified VLAN.

web access interface gre

Supported on: Wi² AP

`web access interface gre <name>`

Enables access to the management tool via the specified GRE tunnel.

`no web access interface gre <name>`

Disables access to the management tool via the specified GRE tunnel.

web access local mesh

Supported on: Wi² AP

`web access local mesh <name>`

Enables access to the management tool via the specified local mesh.

`no web access local mesh <name>`

Disables access to the management tool via the specified local mesh.

clock

Supported on: Wi² AP

`clock <time> <date>`

Sets the system time and date.

Parameters

<time>	**Time as hh:mm:ss. For example: 15:44:00.**
<date>	**Date as dd Month yyyy. For example: 17 Oct 2004**

ntp server

Supported on: Wi² AP

`ntp server <index><host>`

Adds a network time server.

Parameters

<index>	**Index of the time server in the list. Up to 20 time servers are supported. Time servers are checked in the order that they appear in the list.**
<host>	**DNS name or IP address of the time server.**

ntp server failure trap

Supported on: Wi² AP

`ntp server failure trap`

Send a trap each time a time server synchronization failed.

`no ntp server failure trap`

Do not send a trap each time a time server synchronization failed.

config-update automatic

Supported on: Wi² AP

`config-update automatic`

Enables scheduled configuration restore or backup.

`no config-update automatic`

Disables scheduled configuration restore or backup.

The Wi² AP can automatically download the configuration file from a local or remote URL (restore). It is also possible to upload the current configuration to a given URL (backup). Theses operations can be done at preset times.

config-update operation

Supported on: Wi² AP

```
config-update operation (restore | backup)
```

Sets the type of operation that will take place at the preset time.

config-update time

Supported on: Wi² AP

```
config-update time <time>
```

Sets the time of day when the scheduled configuration operation (backup or restore) will take place.

Parameters

<time>	**Time as hh:mm:ss. For example: 15:44:00.**

config-update uri

Supported on: Wi² AP

```
config-update uri <uri>
```

Sets the URI where the Wi² AP will download or upload the configuration file.

```
no config-update uri
```

Clears the configuration file URI.

config-update weekday

Supported on: Wi² AP

```
config-update weekday (everyday | monday | tuesday | wednesday |
thursday | friday | saturday | sunday)
```

Sets the day when the scheduled configuration operation (backup or restore) will take place.

snmp-server trap config-change

Supported on: Wi² AP

```
snmp-server trap config-change
```

Send a trap whenever the configuration is changed.

```
no snmp-server trap config-change
```

Do not send this trap.

snmp-server trap config-update

Supported on: Wi² AP

```
snmp-server trap config-update
```

Send a trap whenever the firmware is updated.

```
no snmp-server trap config-update
```

Do not send this trap.

logging destination

Supported on: Wi² AP

```
logging destination <name>
```

Creates a new remote destination for syslog.

```
no logging destination <name>
```

Deletes the specified syslog destination.

Parameters

<name>	**Name of syslog destination. Use the name "local" to edit your local log file settings. Any other name will edit/create a remote log destination.**

snmp-server trap syslog-severity

Supported on: Wi² AP

```
snmp-server trap syslog-severity
```

Set the severity level of syslog messages that will trigger a trap.

```
no snmp-server trap syslog-severity
```

Do not send this trap.

snmp-server

Supported on: Wi² AP

```
snmp-server
```

Enables the SNMP agent.

```
no snmp-server
```

Disables the SNMP agent.

snmp-server access port-1

Supported on: Wi² AP

```
snmp-server access port-1
```

Enables SNMP access on the downstream port.

```
no snmp-server access port-1
```

Blocks SNMP access on the downstream port.

snmp-server allow

Supported on: Wi² AP

`snmp-server allow <ip address>/<mask>`

Adds a host to the list of IP address from which access to the SNMP interface is permitted.

`no snmp-server allow <ip address>/<mask>`

Removes a host from the list of IP address from which access to the SNMP interface is permitted.

Parameters

<address>	**IP address.**
</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

snmp-server chassis-id

Supported on: Wi² AP

`snmp-server chassis-id <name>`

Specifies a name to identify the Wi² AP. By default, this is set to the serial number of the Wi² AP.

`no snmp-server chassis-id`

Deletes the system name.

snmp-server contact

Supported on: Wi² AP

`snmp-server contact <email>`

Specifies contact information.

`no snmp-server contact`

Deletes contact information.

Parameters

<email>	**Email address.**

snmp-server heartbeat period

Supported on: Wi² AP

`snmp-server heartbeat period <seconds>`

Sets the interval between sending heartbeat traps.

Parameters

<seconds>	**Heartbeat interval in seconds.**

snmp-server location

Supported on: Wi² AP

`snmp-server location <name>`

Specifies the location where the Wi² AP is installed.

`no snmp-server location`

Deletes location information.

Parameters

<name>	**Location where the Wi² AP is installed.**

snmp-server port

Supported on: Wi² AP

`snmp-server port <port number>`

Sets the port the Wi² AP will use to respond to SNMP requests.

Parameters

<port number>	**SNMP port number. Range 1 - 65535.**

snmp-server readonly

Supported on: Wi² AP

`snmp-server readonly <community>`

Sets the read-only community string.

`no snmp-server readonly`

Deletes the read-only community string.

snmp-server readwrite

Supported on: Wi² AP

`snmp-server readwrite <community>`

Sets the read-write community string.

`no snmp-server readwrite`

Deletes the read-write community string.

snmp-server trap

Supported on: Wi² AP

`snmp-server trap`

Enables support for SNMP traps.

`no snmp-server trap`

Disables support for SNMP traps.

snmp-server trap community

Supported on: Wi² AP

`snmp-server trap community <str>`

Sets the password required by the remote host that will receive the trap.

`no snmp-server trap community`

Deletes the password required by the remote host that will receive the trap.

snmp-server trap destination

Supported on: Wi² AP

`snmp-server trap destination <host> <[port number]>`

Add a new trap destination.

`no snmp-server trap destination <host> [<port>]`

Deletes the specified trap destination.

Parameters

<host>	**Sets the IP address or domain name of the host that the Wi² AP will send traps to.**
<[port number]>	**SNMP port number. Range 1 - 65535. By default port 162 is used**

snmp-server trap heartbeat

Supported on: Wi² AP

`snmp-server trap heartbeat`

Enables sending of heartbeat traps at regular intervals.

`no snmp-server trap heartbeat`

Disables sending of heartbeat traps at regular intervals.

snmp-server trap link-state

Supported on: Wi² AP

`snmp-server trap link-state`

Send a trap when the link state changes on any interface.

`no snmp-server trap link-state`

Do not send this trap.

snmp-server trap snmp-authentication

Supported on: Wi² AP

`snmp-server trap snmp-authentication`

Send a trap each time an SNMP request fails to supply the correct community name.

snmp-server version

Supported on: Wi² AP

`snmp-server version (1 | 2c)`

Sets the SNMP version.

snmp-server access interface vlan

Supported on: Wi² AP

`snmp-server access interface vlan <name>`

Enables access to SNMP via the specified VLAN.

`no snmp-server access interface vlan <name>`

Disables access to SNMP via the specified VLAN.

Parameters

<name>	**Specifies the name of the VLAN.**

snmp-server access local mesh

Supported on: Wi² AP

`snmp-server access local mesh <profile>`

Enables access to SNMP via the specified local mesh.

`no snmp-server access local mesh <profile>`

Enables access to SNMP via the specified local mesh.

snmp-server access interface gre

Supported on: Wi² AP

`snmp-server access interface gre <name>`

Enables access to SNMP via the specified GRE tunnel.

`no snmp-server access interface gre <name>`

Removes access to SNMP via the specified GRE tunnel.

snmp-server access wireless

Supported on: Wi² AP

`snmp-server access wireless`

Enables SNMP access on the wireless port.

`no snmp-server access wireless`

Blocks SNMP access on the wireless port.

snmp-server access port-2

Supported on: MWi² AP

`snmp-server access port-2`

Enables SNMP access on the upstream port.

`no snmp-server access port-2`

Blocks SNMP access on the upstream port.

soap-server

Supported on: Wi² AP

`soap-server`

Enables the SOAP server.

`no soap-server`

Disables the SOAP server.

soap-server access interface vlan

Supported on: Wi² AP

`soap-server access interface vlan <name>`

Enables access to SOAP via this VLAN.

`no soap-server access interface vlan <name>`

Disables access to SOAP via this VLAN.

soap-server access port-1

Supported on: Wi² AP

`soap-server access port-1`

Enables SOAP access on the downstream port.

`no soap-server access port-1`

Blocks SOAP access on the downstream port.

soap-server access port-2

Supported on: Wi² AP

`soap-server access port-2`

Enables SOAP access on the upstream port.

`no soap-server access port-2`

Blocks SOAP access on the upstream port.

soap-server allow

Supported on: Wi² AP

`soap-server allow <ip address>/<mask>`

Adds a host to the list of IP address from which access to the SOAP interface is permitted.

`no soap-server allow <ip address>/<mask>`

Removes a host from the list of IP address from which access to the SOAP interface is permitted.

Parameters

<address>	**IP address.**
</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

soap-server http authentication

Supported on: Wi² AP

`soap-server http authentication`

Enable the SOAP server HTTP authentication.

`no soap-server http authentication`

Disable the SOAP server HTTP authentication.

soap-server http authentication password

Supported on: Wi² AP

`soap-server http authentication password`

Set the SOAP server HTTP authentication password.

soap-server http authentication username

Supported on: Wi² AP

`soap-server http authentication username`

Set the SOAP server HTTP authentication username.

soap-server port

Supported on: Wi² AP

`soap-server port <port number>`

Sets the port the Wi² AP will use to respond to SOAP requests.

Parameters

<port number>	**SOAP port number. Range 1 - 65535.**

soap-server ssl

Supported on: Wi² AP

`soap-server ssl`

SSL enabled for SOAP server.

`no soap-server ssl`

SSL disabled for SOAP server.

soap-server ssl with client certificate

Supported on: Wi² AP

`soap-server ssl with client certificate`

Enable the use of client certificate with SSL for SOAP server.

`no soap-server ssl with client certificate`

Disable the use of client certificate with SSL for SOAP server.

soap-server access interface gre

Supported on: Wi² AP

`soap-server access interface gre <name>`

Enables access to SOAP via the specified GRE tunnel.

`no soap-server access interface gre <name>`

Removes access to SOAP via the specified GRE tunnel.

soap-server access wireless

Supported on: Wi² AP

`soap-server access wireless`

Enables SOAP access on the wireless port.

`no soap-server access wireless`

Blocks SOAP access on the wireless port.

soap-server access local mesh

Supported on: Wi² AP

`soap-server access local mesh <profile>`

Enables access to the management tool via the specified local mesh.

`no soap-server access local mesh <profile>`

Disables access to the management tool via the specified local mesh.

snmp-server trap low-snr

Supported on: Wi² AP

`snmp-server trap low-snr`

Send a trap when the average signal to noise ratio on a VAP (virtual network) exceeds a specified level.

`no snmp-server trap low-snr`

Do not send this trap.

snmp-server trap low-snr interval

Supported on: Wi² AP

`snmp-server trap low-snr interval <number>`

Sets the interval at which the average SNR level is checked for each VAP (virtual network).

snmp-server trap low-snr level

Supported on: Wi² AP

`snmp-server trap low-snr level <number>`

Sets the SNR level that will trigger a trap.

snmp-server trap new-association

Supported on: Wi² AP

`snmp-server trap new-association`

Send trap on when a new wireless client station associates with any VAP (VSC).

`no snmp-server trap new-association`

Do not send this trap.

snmp-server trap new-association interval

Supported on: Wi² AP

`snmp-server trap new-association interval <number>`

Interval, in minutes, between notifications.

snmp-server trap vpn-connection

Supported on: Wi² AP

`snmp-server trap vpn-connection`

Send a trap when a customer establishes a VPN connection with the Wi² AP.

`no snmp-server trap vpn-connection`

Do not send this trap.

snmp-server trap wireless-association-fail

Supported on: Wi² AP

`snmp-server trap wireless-association-fail`

Send a trap when a wireless client station fails to associate with the Wi² AP.

`no snmp-server trap wireless-association-fail`

Do not send this trap.

snmp-server trap wireless-association-success

Supported on: Wi² AP

`snmp-server trap wireless-association-success`

Send a trap when a wireless client station successfully associates with the Wi² AP.

`no snmp-server trap wireless-association-success`

Do not send this trap.

snmp-server trap wireless-authentication-fail

Supported on: Wi² AP

```
snmp-server trap wireless-authentication-fail
```

Send a trap when a wireless client station fails to authenticate.

```
no snmp-server trap wireless-authentication-fail
```

Do not send this trap.

snmp-server trap wireless-authentication-success

Supported on: Wi² AP

```
snmp-server trap wireless-authentication-success
```

Send a trap when a wireless client station is successfully associated.

```
no snmp-server trap wireless-authentication-success
```

Do not send this trap.

snmp-server trap wireless-deauthentication-fail

Supported on: Wi² AP

```
snmp-server trap wireless-deauthentication-fail
```

Send a trap when a wireless client station fails to deauthenticate from the Wi² AP.

```
no snmp-server trap wireless-deauthentication-fail
```

Do not send this trap.

snmp-server trap wireless-deauthentication-success

Supported on: Wi² AP

```
snmp-server trap wireless-deauthentication-success
```

Send a trap when a wireless client station deauthenticates from the Wi² AP.

```
no snmp-server trap wireless-deauthentication-success
```

Do not send this trap.

snmp-server trap wireless-disassociation-fail

Supported on: Wi² AP

```
snmp-server trap wireless-disassociation-fail
```

Send a trap when a wireless client station fails to disassociate from the Wi² AP.

```
no snmp-server trap wireless-disassociation-fail
```

Do not send this trap.

snmp-server trap wireless-disassociation-success

Supported on: Wi² AP

```
snmp-server trap wireless-disassociation-success
```

Send a trap when a wireless client station disassociates from the Wi² AP.

```
no snmp-server trap wireless-disassociation-success
```

Do not send this trap.

snmp-server trap wireless-reassociation-fail

Supported on: Wi² AP

```
snmp-server trap wireless-reassociation-fail
```

Send a trap when a wireless client station fails to reassociate with the Wi² AP.

```
no snmp-server trap wireless-reassociation-fail
```

Do not send this trap.

snmp-server trap wireless-reassociation-success

Supported on: Wi² AP

```
snmp-server trap wireless-reassociation-success
```

Send a trap when a wireless client station reassociates with the Wi² AP.

```
no snmp-server trap wireless-reassociation-success
```

Do not send this trap.

snmp-server trap syslog-matches

Supported on: Wi² AP

```
snmp-server trap syslog-matches
```

Send a trap when syslog messages matches a specified regular expression.

```
no snmp-server trap syslog-matches
```

Do not send this trap.

snmp-server trap syslog-matches regex

Supported on: Wi² AP

```
snmp-server trap syslog-matches regex <regex>
```

Sets the regular expression used to match the systlog messages.

snmp-server trap syslog-severity level

Supported on: Wi² AP

```
snmp-server trap syslog-severity level (debug | info | notice |
warning | error | critical | alert | emergency)
```

Set the severity level of syslog messages that will trigger a trap.

snmp-server trap network-trace

Supported on: Wi² AP

```
snmp-server trap network-trace
```

Send a trap when a network trace is started or stopped.

```
no snmp-server trap network-trace
```

Do not send this trap.

firmware-update automatic

Supported on: Wi² AP

```
firmware-update automatic
```

Enables scheduled firmware upgrades.

```
no firmware-update automatic
```

Disables scheduled firmware upgrade.

The Wi² AP can automatically retrieve and install firmware from a local or remote URL at preset times. By placing Wi² AP firmware on a web or ftp server, you can automate the update process for multiple units.

When the update process is triggered the Wi² AP retrieves the first 2K of the firmware file to determine if it is different from the active version. If different, the entire firmware file is then downloaded and installed.

(Different means older or newer. This enables you to return to a previous firmware version if required).

Configuration settings are preserved during the update unless stated otherwise in the release notes for the firmware. However, all active connections will be terminated. Customers will have to log in again after the Wi² AP restarts

firmware-update start

Supported on: Wi² AP

```
firmware-update start
```

Upload the firmware based on a specified URI. This URI can be set with the command: firmware-update uri.

firmware-update time

Supported on: Wi² AP

```
firmware-update time <time>
```

Sets the time of day the scheduled firmware upgrade will take place.

Parameters

<time>	**Time as hh:mm:ss. For example: 15:44:00.**

firmware-update uri

Supported on: Wi² AP

`firmware-update uri <uri>`

Sets the URI where the Wi² AP will retrieve new firmware.

`no firmware-update uri`

Clears the firmware URI.

firmware-update weekday

Supported on: Wi² AP

`firmware-update weekday (everyday | monday | tuesday | wednesday | thursday | friday | saturday | sunday)`

Sets the day when the scheduled firmware upgrade will take place.

snmp-server trap firmware-update

Supported on: Wi² AP

`snmp-server trap firmware-update`

Send a trap on firmware update.

`no snmp-server trap firmware-update`

Do not send a trap on firmware update.

access-controller restrict location

Supported on: Wi² AP

`access-controller restrict location (gateway | mac <mac address>)`

Identifies the access controller the Wi² AP will communicate with.

Parameters

`gateway`	**Use the default gateway as the service controller.**
`mac`	**Use the specified MAC address as the gateway.**
`<mac address>`	**MAC address. Specify 6 pairs of hexadecimal numbers separated by colons, with the values a to f in lowercase. For example: 00:03:52:0a:0f:01**

service-sensor

Supported on: Wi² AP

`service-sensor`

Enables the service sensor. The service sensor polls a target device at present intervals. If the device does not respond, the radio is shut off.

`no service-sensor`

Disables the service sensor.

service-sensor

Supported on: Wi² AP

`service-sensor (gateway | address<ip address>)`

Sets the target device the service sensor will poll. This can be the default gateway or a specific IP address.

`no service-sensor`

Disables the service sensor.

Parameters

`gateway`	**The service sensor will poll the default gateway.**
`address`	**The service sensor will poll another device.**
`<ip address>`	**IP address of the other device. For example: 192.168.10.10**

service-sensor poll

Supported on: Wi² AP

`service-sensor poll <seconds>`

Sets the poll frequency.

Parameters

`<seconds>`	**Poll frequency. Range: 1 - 3600 seconds.**

service-sensor retry

Supported on: Wi² AP

`service-sensor retry <retries>`

Specify how many retries the service sensor will attempt when polling the target device.

When the retry limit is reached, the radio on the Wi² AP is turned off.

Parameters

`<retires>`	**Number of retries. Range: 0 - 100.**

service-sensor timeout

Supported on: Wi² AP

`service-sensor timeout <seconds>`

Sets how long the service sensor will wait for a response to a poll before timing out.

Parameters

`<seconds>`	**Length of timeout. Range: 1 - 5 seconds.**

ip name-server

Supported on: Wi² AP

`ip name-server <primary> [<secondary>]`

Sets the primary and secondary DNS servers overriding dynamically assigned ones.

Parameters

<primary>	**IP address of the primary DNS server.**
<secondary>	**IP address of the secondary DNS server.**

ip name-server cache

Supported on: Wi² AP

`ip name-server cache`

Enables the DNS cache.

`no ip name-server cache`

Disables the DNS cache.

Once a host name has been successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, as the remote DNS server now does not have to be queried for subsequent requests for this host.

The entry stays in the cache until:

- **an error occurs when connecting to the remote host**
- **the time to live (TTL) of the DNS request expires**
- **the Wi² AP is restarted.**

ip name-server dynamic

Supported on: Wi² AP

`ip name-server dynamic`

Enables dynamic assignment of DNS servers.

`no ip name-server dynamic`

Disables dynamic DNS assignment.

ip name-server switch-on-servfail

Supported on: Wi² AP

`ip name-server switch-on-servfail`

Switch to next server when server failure is received.

`no ip name-server switch-on-servfail`

Do not switch to next server when server failure is received.

ip name-server switch-over

Supported on: Wi² AP

`ip name-server switch-over`

Switch over to primary when active.

`no ip name-server switch-over`

Do not switch over to primary when active.

snmp-server trap unauthorized-ap

Supported on: Wi² AP

`snmp-server trap unauthorized-ap`

Send a trap when a rogue access point is detected.

`no snmp-server trap unauthorized-ap`

Do not send this trap.

snmp-server trap unauthorized-ap interval

Supported on: Wi² AP

`snmp-server trap unauthorized-ap interval <number>`

If set to 0, then traps are only sent when a rogue access point is detected. If set to 0, the entire list of rogue access points is sent each time the interval expires.

wireless-scan

Supported on: Wi² AP

`wireless-scan`

Enables wireless neighborhood scanning.

`no wireless-scan`

Disables wireless neighborhood scanning.

wireless-scan period

Supported on: Wi² AP

`wireless-scan period <seconds>`

Specifies the interval between wireless neighborhood scans.

Parameters

<seconds>	**Scanning interval. Range: 10 - 600 seconds.**

wireless-scan url

Supported on: Wi² AP

`wireless-scan url <location>`

Sets the URL of the file that contains a list of all authorized access points.

`no wireless-scan url`

Deletes the URL of the file that contains a list of all authorized access points.

Each entry in the file is composed of two items: MAC address and SSID. Each entry should appear on a new line.

For example:

00:03:52:07:f5:11 "AP_1"

00:03:52:07:f5:23 "AP_2"

00:03:52:07:f5:12 "AP_3"

XML file format is also supported.

access controller shared secret

Supported on: Wi² AP

`access controller shared secret <secret>`

Sets the shared secret used to communicate with the service controller.

`no access controller shared secret`

Sets the shared secret used to communicate with the access controller.

The service controller will only accept authentication/location-aware information from Alvarion satellites that have a matching shared secret to its own.

radius-server profile

Supported on: Wi² AP

`radius-server profile <name>`

Creates a new RADIUS profile or switches to the RADIUS context with the specified profile name.

`no radius-server profile <name>`

Deletes the specified RADIUS profile.

ip-qos profile

Supported on: Wi² AP

`ip-qos profile <name>`

Creates a new IP QoS profile or switches to the IP QoS context with the specified profile name.

`no ip-qos profile <name>`

Deletes the specified IP QoS profile.

dot11 igmp snooping-helper

Supported on: Wi² AP

`dot11 igmp snooping-helper`

Enables IGMP snooping helpers which ensure that the Wi² AP correctly delivers multicast packets to roaming client stations that are part of a multicast group.

`no dot11 igmp snooping-helper`

Disable IGMP snooping helpers.

discovery protocol

Supported on: Wi² AP

`discovery protocol`

Enables broadcast of Alvarion device information for interoperability with CDP-enabled networking hardware.

`no discovery protocol`

Disable broadcast of Alvarion device information.

discovery protocol device-id

Supported on: Wi² AP

`discovery protocol device-id <name>`

Overwrite the device-id field of information packets (the Wi² AP serial number is not used).

`no discovery protocol device-id`

Do not overwrite the device-id field of information packets (use the Wi² AP serial number).

bridge priority

Supported on: Wi² AP

`bridge priority <number>`

Sets the bridge priority for the spanning tree.

The spanning tree uses the bridge ID to elect the root bridge and the designated bridges. The bridge ID is built with the MAC address of the bridge and the bridge priority. The first 2 most significant bytes are the bridge priority and the next 6 bytes are the MAC address. To control which bridge will become the root bridge, you can configure the bridge priority parameter on the bridges. The root will be the bridge with the lowest bridge ID. The Bridge priority has a valid range of 0 to 0xFFFF. The default value is the middle value: 0x8000.

bridge protocol ieee

Supported on: Wi² AP

`bridge protocol ieee`

Enable the bridge spanning tree protocol to prevent undesirable loops from occurring in the network that may result in decreased throughput.

`no bridge protocol ieee`

Disable the bridge spanning tree protocol.

bridge protocol ieee vlan

Supported on: Wi² AP

`bridge protocol ieee vlan`

Enable the bridge spanning tree protocol for VLANs.

`no bridge protocol ieee vlan`

Disable the bridge spanning tree protocol for VLANs.

ip route gateway

Supported on: Wi² AP

`ip route gateway<destination>/<mask> <gateway> <[metric]>`

Adds a static route.

`no ip route gateway <destination>/<mask> <gateway> <[metric]>`

Removes the specified static route.

Parameters

<destination>	**Traffic addressed to this IP address will be routed.**
<mask>	**Indicates the number of bits in the destination address that is checked for a match.**
<gateway>	**Indicates the IP address of the gateway the Wi² AP will forward routed traffic to. The gateway address must be on the same subnet as one of the available interfaces (Internet port or LAN port).**
<metrix>	**Indicates the priority of a route. If two routes exist for a destination address then the Wi² AP chooses the one with the lower metric.**

dot1x reauth

Supported on: Wi² AP

`dot1x reauth`

Enable this option to force 802.1X client stations to reauthenticate.

`no dot1x reauth`

Disables 802.1X reauthentication.

dot1x reauth period

Supported on: Wi² AP

```
dot1x reauth period (15m | 30m | 1h | 2h | 4h | 8h | 12h)
```

Sets the 802.1X reauthentication interval. Client stations must reauthenticate when this interval expires.

dot1x reauth terminate

Supported on: Wi² AP

```
dot1x reauth terminate
```

Enable this option to allow client stations to remain connected during re-authentication. Client traffic is blocked only when re-authentication fails.

```
no dot1x reauth terminate
```

Disabled this option to block client traffic during re-authentication and only activate traffic again if authentication succeeds.

dot1x supplicant timeout

Supported on: Wi² AP

```
802.1x supplicant time-out <seconds>
```

Sets the 802.1X supplicant time-out.

Parameters

<seconds>	**time-out in seconds.**

dynamic key

Supported on: Wi² AP

```
dynamic key
```

Enables dynamic key support for 802.1X and WPA.

```
no dynamic key
```

Disables dynamic key support for 802.1X and WPA.

dynamic key interval

Supported on: Wi² AP

```
dynamic key interval (5m | 10m | 15m | 30m | 1h | 2h | 4h | 8h |
12h)
```

Specifies how often (in minutes or hours) that the group (broadcast) key is changed for 802.1X and WPA.

add wireless ip-qos profile

Supported on: Wi² AP

`add wireless ip-qos profile <name>`

Adds the specified profile to the list of IP QoS profiles in effect for the wireless links.

<profile-name>	**Name of an existing IP QoS profile.**

delete wireless ip-qos profile all

Supported on: Wi² AP

`delete wireless ip-qos profile all`

Clears the list of IP QoS profiles currently in effect for the wireless links.

delete wireless ip-qos profile

Supported on: Wi² AP

`delete wireless ip-qos profile <name>`

Removes the specified profile from the list of IP QoS profiles in effect for the wireless links.

<profile-name>	**Name of an existing IP QoS profile currently in the profile list for the wireless links.**

wireless link qos

Supported on: Wi² AP

`wireless link qos (disabled | 802.1p | wme | very-high | high | normal | low | tos | diffsrv)`

Sets the wireless link QoS policy.

sensor discovery mode

Supported on: Wi² AP

`sensor discovery mode (id | ip)`

Sets the method the Wi² AP will use to communicate with the RF Manager Server.

Parameters

`id`	**Connect using the Server ID of the RF Manager Server.**
`ip`	**Connect using the IP address or hostname of the RF Manager Server.**

Description

For these methods to work, the following must be true:

• The Wi² AP must be able to reach the RF Manager Server via a network connected to port 1 or port 2. For example, you should be able to ping the RF Manager Server,Äôs IP address from the Wi² AP.

• If there are any firewalls between the Wi² AP and the RF Manager Server, then TCP and UDP ports 3851 must be open bi-directionally.

• If using the hostname option, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.

• If using the Server ID option, support for multicast traffic must be enabled on all routers and switches connected between the Wi² AP and the RF Manager Server.

sensor network detector

Supported on: Wi² AP

```
sensor network detector
```

Enable the Network Detector.

```
no sensor network detector
```

Disable the Network Detector.

sensor server id

Supported on: Wi² AP

```
sensor server id <id>
```

Sets the server ID of the the RF Manager Server to connect to.

Parameters

ID	**Specify the Server ID of the RF Manager Server to connect to. Set the Server ID to 0 to have the Wi² AP send a discovery request to all active Alvarion InCharge RF Manager Servers. The Wi² AP will connect to the first server that responds to the discovery request.**

sensor server name

Supported on: Wi² AP

```
sensor server name <name>
```

Sets the IP address or hostname of the the RF Manager Server to connect to.

Parameters

Name	**Specify the IP address of the the RF Manager Server or its hostname. If a hostname is specified, the Wi² AP must be able to resolve it via DNS,Äîthat is, an entry must be created on the network DNS server that points to the IP address of the RF Manager Server.**

config-version

Supported on: Wi² AP

```
config-version <string>
```

Sets a string to identify the user configuration version.

2.4 Port-2 Interface Context

Context path: View > Enable > Config > Port-2 interface

This context provides commands for configuring Port-2.

duplex

Supported on: Wi² AP

`duplex (auto | half | full)`

Sets the duplex mode on Port-2.

Parameters

`auto`	**Lets the Wi² AP automatically set duplex mode based on the type of equipment it is connected to.**
`half`	**Forces the port to operate in half duplex mode.**
`full`	**Forces the port to operate in full duplex mode.**

end

Supported on: Wi² AP

`end`

Switches to parent context.

speed

Supported on: Wi² AP

`speed (auto | 10 | 100)`

Sets the speed of Port-2.

Parameters

`auto`	**Lets the Wi² AP automatically set port speed based on the type of equipment it is connected to.**
`100`	**Forces the port to operate at 100 mbps.**
`10`	**Forces the port to operate at 10 mbps.**

vlan

Supported on: Wi² AP

`vlan <id>`

Sets the default VLAN ID. Range: 1 - 4094. All outgoing traffic that does not have a VLAN already assigned to it, is sent on this VLAN.

`no vlan`

Deletes the default VLAN ID.

vlan compatibility mode

Supported on: Wi² AP

`vlan compatibility mode`

When this option is enabled, the Wi² AP sends all management traffic AND all untagged traffic on both the default VLAN and untagged.

`no vlan compatibility mode`

Disable VLAN and untagged compatibility mode.

vlan-management filter

Supported on: Wi² AP

`vlan-management filter`

Restricts the default VLAN to carry management traffic only.

`no vlan-management filter`

Does not restrict the default VLAN to carry management traffic only.

Management traffic includes:

- **all traffic that is exchanged by the Wi² AP and the access controller**
- **all communications with RADIUS servers**
- **HTTPS sessions to the management tool**
- **SNMP traffic**

interface vlan

Supported on: Wi² AP

`interface vlan <id>[-<id2>]`

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

`no interface vlan <id>[-<id2>]`

Deletes the specified VLAN.

Parameters

<id>	**VLAN ID. Range: 1 - 4094.**
<id2>	**VLAN ID. When specified, this is the last value in a range.**

2.5 Port-1 Interface Context

Context path: View > Enable > Config > Port-1 interface

This context provides commands for configuring Port-1.

duplex

Supported on: Wi² AP

`duplex (auto | half | full)`

Sets the duplex mode on Port-1.

Parameters

`auto`	**Lets the Wi² AP automatically set duplex mode based on the type of equipment it is connected to.**
`half`	**Forces the port to operate in half duplex mode.**
`full`	**Forces the port to operate in full duplex mode.**

end

Supported on: Wi² AP

`end`

Switches to parent context.

speed

Supported on: Wi² AP

`speed (auto | 10 | 100)`

Sets the speed of Port-1.

Parameters

`auto`	**Lets the Wi² AP automatically set port speed based on the type of equipment it is connected to.**
`100`	**Forces the port to operate at 100 mbps.**
`10`	**Forces the port to operate at 10 mbps.**

vlan

Supported on: Wi² AP

`vlan <id>`

Sets the default VLAN ID. Range: 1 - 4094. All outgoing traffic that does not have a VLAN already assigned to it, is sent on this VLAN.

`no vlan`

Deletes the default VLAN ID.

vlan compatibility mode

Supported on: Wi² AP

`vlan compatibility mode`

When this option is enabled, the Wi² AP sends all management traffic AND all untagged traffic on both the default VLAN and untagged.

`no vlan compatibility mode`

Disable VLAN and untagged compatibility mode.

vlan-management filter

Supported on: Wi² AP

`vlan-management filter`

Restricts the default VLAN to carry management traffic only.

`no vlan-management filter`

Does not restrict the default VLAN to carry management traffic only.

Management traffic includes:

- **all traffic that is exchanged by the Wi² AP and the access controller**
- **all communications with RADIUS servers**
- **HTTPS sessions to the management tool**
- **SNMP traffic**

interface vlan

Supported on: Wi² AP

`interface vlan <id>[-<id2>]`

Switches to the specified VLAN interface or create a new VLAN interface with the specified ID.

`no interface vlan <id>[-<id2>]`

Deletes the specified VLAN interface.

Parameters

<id>	**VLAN ID. Range: 1 - 4094.**
<id2>	**VLAN ID. When specified, is the last value in a range.**

2.6 WAN IP Interface Context

Context path: View > Enable > Config > WAN IP interface

This context provides commands for configuring various IP-networking related settings.

pppoe client user

Supported on: Wi² AP

`pppoe client user <username> <password>`

Sets the PPPoE username and password.

`no pppoe client user`

Deletes the PPPoE username.

Parameters

<username>	**The username assigned to you by your ISP. The Wi² AP will use this username to log on to your ISP when establishing a PPPoE connection.**
<password>	**The password assigned to you by your ISP. The Wi² AP will use this username to log on to your ISP when establishing a PPPoE connection.**

ip address mode

Supported on: Wi² AP

`ip address mode (dhcp | pppoe | static)`

Sets the IP addressing mode for Port-2.

Parameters

`dhcp`	**Dynamic host configuration protocol. The DHCP server will automatically assign an address to the Wi² AP, which functions as a DHCP client.**
`pppoe`	**Point-to-point protocol over Ethernet. The PPPoE server will automatically assign an IP address to the Wi² AP. You need to supply a username and password so the Wi² AP can log on.**
`static`	**This option enables you to manually assign an IP address to the Wi² AP.**

ip address

Supported on: Wi² AP

`ip address <ip address>/<mask>`

Sets a static IP address for the port.

Parameters

<address>	**IP address.**

</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

ip address dhcp client-id

Supported on: Wi² AP

`ip address dhcp client-id <id>`

Specifies an ID to identify the Wi² AP to a DHCP server. This parameter is not required by all ISPs.

`no ip address dhcp client-id`

Deletes the specified DHCP client id.

end

Supported on: Wi² AP

`end`

Switches to parent context.

pppoe auto-reconnect

Supported on: Wi² AP

`pppoe auto-reconnect`

The Wi² AP will automatically attempt to reconnect if the connection is lost.

`no pppoe auto-reconnect`

The Wi² AP will not automatically attempt to reconnect if the connection is lost.

pppoe mru

Supported on: Wi² AP

`pppoe mru <bytes>`

Specifies the maximum receive unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	**Maximum size (in bytes) of a PPPoE packet when receiving. Range: 500 - 1500 bytes.**

pppoe mtu

Supported on: Wi² AP

`pppoe mtu <bytes>`

Specifies the maximum transmit unit.

Changes to this parameter should only be made according to the recommendations of your ISP. Incorrectly setting this parameter can reduce the throughput of your Internet connection.

Parameters

<bytes>	**Maximum size (in bytes) of a PPPoE packet when transmitting. Range: 500 - 1500 bytes.**

pppoe unnumbered

Supported on: Wi² AP

```
pppoe unnumbered
```

Enable unnumbered mode.

```
no pppoe unnumbered
```

Disable unnumbered mode.

This feature is useful when the Wi² AP is connected to the Internet and NAT is not being used. Instead of assigning two IP addresses to the Wi² AP, one to the Internet port and one to the LAN port, both ports can share a single IP address. This is especially useful when a limited number of IP addresses are available to you.

2.7 Wireless Context

Context path: View > Enable > Config > Wireless

This context provides commands for configuring the wireless network.

end

Supported on: Wi² AP

`end`

Switches to parent context.

radio active

Supported on: Wi² AP

`radio active`

Enables the radio.

`no radio active`

Disables the radio.

rts threshold

Supported on: Wi² AP

`rts threshold <value>`

Sets the RTS threshold.

`no rts threshold`

Deletes the RTS threshold value.

Parameters

< value>	**Threshold value in the range 128 and 1540.**

Description

Use this parameter to control collisions on the link that can reduce throughput. If the Status Wireless page on the management tool shows increasing values for Tx multiple retry frames or Tx single retry frames, you should adjust this value until the errors clear up. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated.

Using a small value for RTS threshold can affect throughput.

If a packet is larger than the threshold, the Wi² AP will hold it and issue a request to send (RTS) message to the client station. Only when the client station replies with a clear to send (CTS) message will the Wi² AP send the packet. Packets smaller than the threshold are transmitted without this handshake.

distance

Supported on: Wi² AP

`distance (small | medium | large)`

Sets the distance between access points.

Use this parameter to adjust the receiver sensitivity of the Wi² AP. This parameter should only be changed if:

- **you have more than one wireless access point installed in your location**
- **you are experiencing throughput problems**

In all other cases, use the default setting of Large.

If you have installed multiple Wi² APs, reducing the receiver sensitivity of the Wi² AP from its maximum will help to reduce the amount of crosstalk between the wireless stations to better support roaming clients. By reducing the receiver sensitivity, client stations will be more likely to connect with the nearest access point.

dot11

Supported on: Wi² AP

`dot11 <mode> <frequency>`

Sets the wireless mode and the frequency the Wi² AP will operate at.

Parameters

<mode>

Sets the transmission speed and frequency band. The available options are determined by the wireless card installed in the Wi² AP, and may include:

- **b: Selects 802.11b providing 11 Mbps in the 2.4 GHz frequency band.**
- **g: Selects 802.11g providing 54 Mbps in the 2.4 GHz frequency band.**
- **bg: Selects 802.11b + 802.11g providing 11 and 54 Mbps in the 2.4 GHz frequency band.**

<frequency>

Sets the operating frequency by specifying a number in GHz or by specifying a channel number. The frequencies that are available are determined by the radio installed in the Wi² AP and the regulations that apply in your country.

For optimum performance when operating in 802.11b or 802.11g modes, choose a frequency that differs from other wireless access points operating in neighboring cells by at least 25 MHz.

transmit power

Supported on: Wi² AP

`transmit power (DB | max)`

Sets the maximum transmission power of the wireless radio.

Parameters

<*db*>	**Power is specified in steps of 1dBm. The maximum setting is 18 dBm.**

Note: The actual transmit power used may less than the value specified. The Wi² AP determines the power to used based on the settings you made for regulatory domain, wireless mode, and operating frequency.

antenna bidirectionnal

Supported on: Wi² AP

```
antenna bidirectionnal (diversity | main | auxiliary)
```

Sets the antenna to transmit and receive on. Select diversity to transmit and receive on both antennas.

Parameters

`diversity`	**In this mode both antennas are used to transmit and receive. The Wi² AP supports both transmit and receive diversity.**
`main`	**Transmit and receive on the main antenna only.**
`aux`	**Transmit and receive on the aux antenna only.**

autochannel skip

Supported on: Wi² AP

```
autochannel skip <chan>
```

Adds the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

```
no autochannel skip <chan>
```

Removes the specified channel to the list of channels that are not allowed to be selected by the Auto Channel algorithm.

beacon interval

Supported on: Wi² AP

```
beacon interval <value>
```

Sets the beacon interval.

Parameters

< *value*>	**Beacon interval value in the range 20 and 500 time units (TU) (1 TU = 1024us).**

dot11 automatic frequency

Supported on: Wi² AP

```
dot11 automatic frequency
```

Enable this option to have the Wi² AP automatically determine the best operating frequency.

```
no dot11 automatic frequency
```

Disable automatic frequency selection.

dot11 automatic frequency period

Supported on: Wi² AP

```
dot11 automatic frequency period (disabled | 1h | 2h | 4h | 8h | 12h | 24h)
```

Specify how often the frequency setting is re-evaluted when automatic frequency selection is enabled.

dot11 automatic frequency time

Supported on: Wi² AP

```
dot11 automatic frequency time <time>
```

Specify when the channel should be re-evaluated.

dot11 automatic transmit-power

Supported on: Wi² AP

```
dot11 automatic transmit-power
```

Enables automatic transmit power selection.

```
no dot11 automatic transmit-power
```

Disables automatic transmit power selection.

dot11 automatic transmit-power period

Supported on: Wi² AP

```
dot11 automatic transmit-power period (1h | 2h | 4h | 8h | 12h | 24h)
```

Sets the interval at which the transmit power setting is re-evaluated when automatic power selection is enabled.

multicast rate

Supported on: Wi² AP

```
multicast rate (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)
```

Sets the transmit rate for multicast traffic.

This is a fixed rate, which means that if a station is too far away to receive traffic at this rate, then the multicast will not be seen by the station. By rasing the multicast rate you can increase overall throughput significantly.

station distance

Supported on: Wi² AP

```
station distance (0km | 5km | 10km | 15km | 20km | 25km | 30km | 35km)
```

Fine tunes internal timeout settings to account for the distance that wireless links span. For normal operation, the CNx is optimized for links of less than 1 km.

This is a global setting that is useful when creating wireless links to remote sites. However, it also applies to all wireless connection made with the radio, not just for wireless links. Therefore, if you are also using the radio to serve local wireless client stations, adjusting this setting may lower the performance for clients with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)

dot11 mode

Supported on: Wi² AP

```
dot11 mode (monitor | ap+wds | ap-only | wds-only | sensor)
```

Sets the operating mode for the radio.

bandwidth

Supported on: Wi² AP

```
bandwidth
```

Enables bandwidth control.

```
no bandwidth
```

Disables bandwidth control.

bandwidth max

Supported on: Wi² AP

```
bandwidth max <rate>
```

Set the maximum data rate on the wireless port in kbps.

Parameters

<rate>	**Maximum data rate. Range: 500 - 54000 kbps.**

2.8 Virtual AP Context

Context path: View > Enable > Config > Virtual AP

This context provides commands for configuring Virtual AP profiles (VAP (VSC)s).

By default one profile exists with the name "Alvarion Networks". This is the default profile and cannot be deleted.

The following example shows how to add a new VAP (VSC) with egress mapped to an existing VLAN named "hongkong":

CLI(config)# virtual ap newap

CLI(virtual-ap)# access control

CLI(virtual-ap)# egress any vlan hongkong

CLI(virtual-ap)# ssid name "newap"

CLI(virtual-ap)# ingress ssid

CLI(virtual-ap)# bandwidth high

CLI(virtual-ap)# end

CLI(config)#

---

virtual ap name

Supported on: Wi² AP

`virtual ap name <name>`

Change the VAP (VSC) name.

---

access controller

Supported on: Wi² AP

`access controller`

Use the services of an access controller for authentication and control of client sessions.

`no access controller`

Do not use the services of an access controller for authentication and control of client sessions.

---

ingress interface

Supported on: Wi² AP

`ingress interface (wireless | wireless) <name>`

Sets the specified interface as the ingress interface traffic will be accepted on.

`no ingress interface (wireless | wireless) <name>`

Removes the specified interface as an ingress interface.

max-association

Supported on: Wi² AP

`max-association <stations>`

Sets the maximum number of clients stations that can associate with this VAP (VSC).

<stations>	**Number of client stations. Range: 1 - 255.**

ssid name

Supported on: Wi² AP

`ssid name <name>`

Specifies the WLAN name (SSID) for the profile.

vlan

Supported on: Wi² AP

`vlan <id>`

Assigns a VLAN ID to this VAP (VSC).

`no vlan`

Deletes the VLAN ID for this VAP (VSC).

Parameters

<id>	**VLAN ID. Range: 1 - 4094.**

guest-mode

Supported on: Wi² AP

`guest-mode`

Enables broadcast of the wireless network name (SSID).

`no guest-mode`

Disables broadcast of the wireless network name (SSID).

encryption key 1

Supported on: Wi² AP630

`encryption key <key> <value>`

Sets WEP key 1.

`no encryption key <key>`

Deletes WEP key 1.

Parameters

<key>	**WEP key number. Range: 1 - 4. Keys 2 to 4 are only supported on the first WLAN profile.**

<value>	**Key value. The number of characters you specify for a key determines the level of encryption the Wi² AP will provide.** **For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits.** **For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.**

encryption key format

Supported on: Wi² AP

`encryption key format (hex | ascii)`

Specify the WEP key format.

Parameters

`hex`	**Hex keys should only include the following digits: 0-9, a-f, A-F**
`ascii`	**ASCII keys are much weaker than carefully chosen hex keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.**

transmit key

Supported on: Wi² AP

`transmit key <key number>`

Sets the key the Wi² AP will use to encrypt transmitted data. All four keys are used to decrypt received data.

Parameters

<key number>	**Transmit key number. Range: 1 -4.**

authentication server access controller

Supported on: Wi² AP

`authentication server access controller`

Use the access controller to authenticate 802.1x or WPA logins.

authentication server accounting

Supported on: Wi² AP

`authentication server accounting`

Enables RADIUS accounting for this VAP (VSC).

`no authentication server accounting`

Disables RADIUS accounting for this VAP (VSC).

authentication server accounting radius profile

Supported on: Wi² AP

`authentication server accounting radius profile <name>`

Sets RADIUS accounting to use the specified RADIUS profile.

`no authentication server accounting radius profile`

Removes accounting support for 802.1x.

authentication server radius

Supported on: Wi² AP

`authentication server radius <name>`

Sets the RADIUS profile to use for 802.1x or WPA authentication.

wpa-psk

Supported on: Wi² AP

`wpa-psk <key>`

Sets the WPA preshared key.

`no wpa-psk`

Deletes the WPA preshared key.

Parameters

`password`	**Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers.**

Description

The Wi² AP uses the key you specify to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as using dynamically generated keys.

authentication server accounting radius stationid case

Supported on: Wi² AP

`authentication server accounting radius stationid case (uppercase | lowercase)`

Specifies the case applied to the station delimiter if it is a letter.

authentication server accounting radius stationid delimiter

Supported on: Wi² AP

`authentication server accounting radius stationid delimiter (null | colon | dash | dot | space | comma | under)`

Specifies the one-character delimiter that will be used to format both the calling station ID and the called station ID attributes in RADIUS packets.

wireless filters

Supported on: Wi² AP

`wireless filters`

Enables the wireless security filters which only allow traffic to flow between the Wi² AP and a specific upstream device (such as a Alvarion service controller).

`no wireless filters`

Do not limit traffic flow between the Wi² AP and an upstream device.

This prevents wireless customers from accessing resources on the backbone LAN that interconnects the Wi² AP and the upstream device.

wireless filters mac

Supported on: Wi² AP

`wireless filters mac <mac>`

Sets the MAC address of the upstream device to send traffic to.

`no wireless filters mac <mac>`

Deletes the MAC address of the upstream device to send traffic to.

wireless filters rule input

Supported on: Wi² AP

`wireless filters rule input <rule>`

Adds a custom filter definition for incoming wireless traffic.

Use this command to define custom security filters for incomming wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few Alvarion-specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the Wi² AP when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- **%a - MAC address of the access controller.**
- **%b - MAC address of the bridge.**
- **%g - Mac address of the default gateway assigned to the Wi² AP.**
- **%w - MAC address of wireless port.**

wireless filters rule output

Supported on: Wi² AP

`wireless filters rule output <rule>`

Adds a custom filter definition for outgoing wireless traffic.

Use this command to define custom security filters for outgoing wireless traffic. Filters are specified using standard pcap syntax (http://www.tcpdump.org/tcpdump_man.html) with the addition of a few Alvarion-specific placeholders. These placeholders can be used to refer to specific MAC addresses and are expanded by the Wi² AP when the filter is activated. Once expanded, the filter must respect the pcap syntax. The pcap syntax is documented in the tcpdump man page:

Placeholders

- **%a - MAC address of the access controller.**
- **%b - MAC address of the bridge.**
- **%g - Mac address of the default gateway assigned to the Wi² AP.**
- **%w - MAC address of wireless port.**

wireless filters type

Supported on: Wi² AP

```
wireless filters type (mac | gateway | rules)
```

Sets the type of wireless security filter to use.

Parameters

`mac`	**Traffic is forwarded to an upstream device with a specifiec MAC address. Wireless security filters use the default definitions.**
`gateway`	**Traffic is forwarded to the default gateway assigned to the Wi² AP. Wireless security filters use the default definitions.**
`custom`	**Lets you define custom security filters and address for the upstream device.**

Description

TheWi² AP features an intelligent bridge which can apply security filters to safeguard the flow of wireless traffic. The filters limit both incoming and outgoing traffic as defined below, and force the Wi² AP to exchange traffic with a specific upstream device. If the Wi² AP is configured to use the services of a Alvarion access controller, then the default security filters are automatically enabled and all traffic is sent to the access controller.

Default filters for incoming wireless traffic

Applies to traffic sent from wireless client stations to the CNx.

Accepted

- **Any IP traffic addressed to the access controller.**
- **PPPoE traffic (The PPPoe server must be the upstream device.)**
- **IP broadcast packets, except NetBIOS**
- **Certain address management protocols (ARP, DHCP) regardless of their source address.**
- **Any traffic addressed to the CNx, including 802.1x.**

Blocked

• All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address. TTPS traffic not addressed to the CNx (or upstream device) is also blocked, which means wireless client stations cannot access the management tool on other Alvarion products.

Default filters for outgoing wireless traffic

Applies to traffic sent from the CNx to wireless client stations.

Accepted

• Any IP traffic coming from the upstream device, except NetBIOS packets.

• PPPoE traffic from the upstream device.

• IP broadcast packets, except NetBIOS

• ARP and DHCP Offer and ACK packets.

• Any traffic coming from the CNx itself, including 802.1x.

Blocked

• All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address.

---

mac-filters local

Supported on: Wi² AP

`mac-filters local`

Enables the MAC filter list.

`no mac-filters local`

Disables the MAC filter list.

---

mac-filters

Supported on: Wi² AP

`mac-filters <address>`

Adds an address to the MAC filter list.

`no mac-filters <address>`

Remove the specified address from the MAC filter list.

Parameters

<address>	**MAC address. Specify 6 pairs of hexadecimal numbers separated by colons, with the values a to f in lowercase. For example: 00:03:52:0a:0f:01**

Description

This feature enables you to control access to the Wi² AP based on the MAC address of client stations. You can either block access or allow access, depending on your requirements. When both this option and the MAC-based authentication options are enabled, the following applies: if a customer‚Äôs MAC address does not appear in the MAC filtering list, then MAC-based authentication takes place for that customer.

mac-filters mode

Supported on: Wi² AP

`mac-filters mode (allow | block)`

Either allow or block access to the wireless network for client stations whose addresses appear in the MAC filter list.

mac authentication accounting

Supported on: Wi² AP

`mac authentication accounting`

Enables RADIUS accounting for this VAP (VSC).

`no mac authentication accounting`

Disables RADIUS accounting for this VAP (VSC).

mac authentication accounting radius profile

Supported on: Wi² AP

`mac authentication accounting radius profile <name>`

Sets RADIUS accounting to use the specified RADIUS profile.

`no mac authentication accounting radius profile`

Disables accounting support for MAC authentication.

mandatory authentication

Supported on: Wi² AP

`mandatory authentication`

MAC-based authentication is mandatory.

`no mandatory authentication`

MAC-based authentication is not mandatory.

mac authentication radius profile

Supported on: Wi² AP

`mac authentication radius profile <radiusname>`

Specifies the name of the RADIUS profile to use for MAC-based authentication.

`no mac authentication radius profile`

Do not use a RADIUS profile.

mac authentication radius stationid case

Supported on: Wi² AP

`mac authentication radius stationid case (uppercase | lowercase)`

Specifies the case applied to the station delimiter if it is a letter.

mac authentication radius stationid delimiter

Supported on: Wi² AP

`mac authentication radius stationid delimiter (null | colon | dash | dot | space | comma | under)`

Specifies the one-character delimiter that will be used to format both the calling station ID and the called station ID attributes in RADIUS packets.

mac authentication

Supported on: Wi² AP

`mac authentication`

Enables support for MAC-based authentication.

`no mac authentication`

Disable support for MAC-based authentication.

dot1x mandatory authentication

Supported on: Wi² AP

`dot1x mandatory authentication`

Authentication is mandatory.

`no dot1x mandatory authentication`

Authentication is not mandatory.

add ip filter

Supported on: Wi² AP

`add ip filter <ip address>/<mask>`

Adds an IP filter to the list of destination addresses that traffic will be accepted for. All other traffic will be blocked.

If the list is empty, then all wireless-to-wired LAN traffic is permitted.

Where:

<address>	**IP address.**
</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

delete ip filter

Supported on: Wi² AP

`delete ip filter <ip address>/<mask>`

Deletes the specified address from the IP filter list.

If the list is empty, then all wireless-to-wired LAN traffic is permitted.

Where:

<address>	**IP address.**

</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

delete ip filter all

Supported on: Wi² AP

`delete ip filter all`

Deletes all addresses from the IP filter list.

ip filters

Supported on: Wi² AP

`ip filters`

Activates the IP filter which enables you to block wireless-to-wired LAN traffic on this profile based on its destination address.

`no ip filters`

Disables the IP filter for this profile.

active

Supported on: Wi² AP

`active`

Enable this VAP (virtual network).

`no active`

Disable this VAP (virtual network).

beacon dtim count

Supported on: Wi² AP

`beacon dtim count <number>`

Defines the DTIM period in the beacon.

Client stations use the DTIM to wake up from low-power mode to receive multicast traffic. The Wi² AP transmits a beacon every 100 ms. The DTIM counts down with each beacon that is sent, therefore if the DTIM is set to 5, then client stations in low-power mode will wake up every 500 ms (.5 second) to receive multicast traffic.

public forwarding

Supported on: Wi² AP

`public forwarding (any | 802.1x | none)`

Enables support for traffic exchange between wireless client stations.

fast authentication

Supported on: Wi² AP

```
fast authentication
```

Enables WPA2 opportunistic key caching.

```
no fast authentication
```

Disables WPA2 opportunistic key caching.

layer3 mobility

Supported on: Wi² AP

```
layer3 mobility
```

Enables Layer 3 mobility.

```
no layer3 mobility
```

Disables Layer 3 mobility.

beacon transmit power

Supported on: Wi² AP

```
beacon transmit power
```

Advertise the current transmit power setting in the beacon.

```
no beacon transmit power
```

Do not advertise the current transmit power setting in the beacon.

data rate maximum

Supported on: Wi² AP

```
data rate maximum (1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48
| 54 | highest)
```

Sets the maximum transmission rate that clients stations must respect in order to connect with this SSID. Clients stations that attempt to associate at a higher data rate will be refused. Select the Highest option to have the Wi² AP automatically adjust the data rate to its maximum setting based on the wirelessmode being used.

data rate minimum

Supported on: Wi² AP

```
data rate minimum (lowest | 1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24
| 36 | 48 | 54)
```

Sets the minimum transmission rate that clients stations must meet in order to connect with this SSID. Client stations that are below this setting will not be able to connect to this SSID. Set the Lowest option to have the Wi² AP automatically adjust the data rate to its minimum setting based on the wirelessmode being used.

add ip-qos profile

Supported on: Wi² AP

```
add ip-qos profile <name>
```

Adds the specified profile to the list of IP QoS profiles in effect for this VAP (VSC).

<profile-name>	**Name of an existing IP QoS profile.**

delete ip-qos profile all

Supported on: Wi² AP

```
delete ip-qos profile all
```

Clears the list of IP QoS profiles currently in effect for this VAP (VSC).

delete ip-qos profile

Supported on: Wi² AP

```
delete ip-qos profile <name>
```

Removes the specified profile from the list of IP QoS profiles in effect for this VAP (VSC).

<profile-name>	**Name of an existing IP QoS profile currently in the profile list for this VAP (VSC).**

qos

Supported on: Wi² AP

```
qos ( 802.1p | very-high | high | normal | low | diffsrv | tos |
default | vap0 | vap1 | vap2 | vap3)
```

Sets the QoS level for this profile.

```
no qos
```

Disables QoS for this profile.

Four traffic queues are provided based on the WME standard. In order of priority, these queues are:

- **1: Voice traffic**
- **2: Video traffic**
- **3: Best effort data traffic**
- **4: Background data traffic**

Each QoS priority mechanism maps traffic to one of the four traffic queues. Client stations that do not support the QoS mechanism for the profile they are connected to are always assigned to queue 3.

Important: Traffic delivery is based on strict priority (per the WME standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

802.1p	**Traffic from 802.1p client stations is classified based on the VLAN priority field present within the VLAN header. When this mechanism is selected, the Wi² AP will advertise WME capabilities, enabling WME clients to associate and take advantage of them. This setting has no effect on legacy clients.** **Note: To support 802.1p, the wireless profile must have a VLAN assigned to it, which means that client station traffic is forwarded onto the LAN port only.**
vap0 to vap3	**Allows a specific priority level to be specified for all traffic on a VAP (VSC) profile. This enables client stations without a QoS mechanism to set traffic priority by connecting to the appropriate SSID.** **If you enable this priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set SSID-based low priority for a profile, all devices that connect to the profile have their traffic set at this priority** **Mapping to the traffic queues is as follows: vap0 or very-high=queue 1, vap1 or high=queue 2, vap2 or normal=queue 3, vap3 or low=queue 4**
diffsrv	**Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which the CN320 maps to the appropriate traffic queue. (default setting)**
tos	**The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.**

upstream diffserv tagging

Supported on: Wi² AP

```
upstream diffserv tagging
```

Enables upstream diffserv tagging.

```
no upstream diffserv tagging
```

Disables upstream diffserv tagging.

wmm advertising

Supported on: Wi² AP

```
wmm advertising
```

Enables WMM information element advertising.

```
no wmm advertising
```

Disables WMM information element advertising.

location-aware group

Supported on: Wi² AP

`location-aware group <name>`

Sets the specified group name for the access point.

`no location-aware group`

Deletes the specified group name for the access point.

end

Supported on: Wi² AP

`end`

Switches to parent context.

security

Supported on: Wi² AP

`security (none | wep | 802.1x [wep | static-wep] | wpa (psk | radius) [ v1 | v2 ] )`

Sets the current wireless security policy.

Parameters

`none`	**No wireless security.**
`wep`	**This option enables support for wireless users with WEP client software.**
`802.1x`	**This option enables support for wireless users with 802.1X client software. The Wi² AP supports 802.1x client software that uses EAP-TLS, EAP-TTLS, EAP-SIM, and PEAP.**
`wep`	**Enables the use of dynamic WEP keys for all 802.1X sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pairwise key. It is automatically generated by the Wi² AP.**
`static-wep`	**Support client stations using static WEP keys.**
`wpa`	**This option enables support for wireless users with WPA client software.**
`psk`	**Enables support for a preshared key:**
`radius`	**The Wi² AP obtains the MPPE key from the RADIUS server. This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream.**
`v1,v2`	**Specify which version of WPA to use. None will use both versions (mixed mode).**

2.9 VLAN interface Context

Context path: View > Enable > Config > Port-2 interface > VLAN interface
View > Enable > Config > Port-1 interface > VLAN interface
View > Enable > Config > Local mesh > VLAN interface

This context provides commands for configuring Virtual LANs (VLANs). In this context, VLANs can be added or edited.

For example, to create a new VLAN interface named "hongkong" on the LAN port with VLAN id 88, do the following:

CLI(config)# interface lan

CLI(if-lan)# interface vlan 88

CLI(if-vlan)# vlan name hongkong

CLI(if-vlan)# ip address mode dhcp

CLI(if-vlan)# no nat

CLI(if-vlan)# end

CLI(if-lan)#

end

Supported on: Wi² AP

`end`

Switches to parent context.

ip address

Supported on: Wi² AP

`ip address <ip address>/<mask>`

Sets a static IP address for the VLAN.

Parameters

<address>	**IP address.**
</mask>	**Subnet mask in CIDR format. Specifies the number of bits in the mask.**

ip address mode

Supported on: Wi² AP

`ip address mode (dhcp | static | none)`

Sets the IP addressing mode for this VLAN interface.

Parameters

`dhcp`	**Dynamic host configuration protocol. The DHCP server will automatically assign an address to the Wi² AP, which functions as a DHCP client.**

`static`	**This option enables you to manually assign an IP address to the Wi² AP.**
`none`	**This VLAN does not have an IP address.**

vlan name

Supported on: Wi² AP

`vlan name <name>`

Change the name of this VLAN interface.

2.10 Local Mesh Context

Context path: View > Enable > Config > Local mesh

This context provides commands for configuring local meshes.

end

Supported on: Wi² AP

`end`

Switches to parent context.

active

Supported on: Wi² AP

`active`

Activates the local mesh.

`no active`

Deactivates the local mesh.

interface

Supported on: Wi² AP

`interface (radio1 | radio2 | radio3)`

Select the interface to which this local mesh link applies.

`no interface (radio1 | radio2 | radio3)`

Select the interface to remove for this local mesh link.

local mesh name

Supported on: Wi² AP

`local mesh name <name>`

Renames the current local mesh link.

remote mac

Supported on: Wi² AP

`remote mac <address>`

Sets the MAC address of the remote access point.

`no remote mac`

Deletes the MAC address of the remote access point.

Parameters

<address>	**MAC address. Specify 6 pairs of hexadecimal numbers separated by colons, with the values a to f in lowercase. For example: 00:03:52:0a:0f:01**

security

Supported on: Wi² AP

`security`

Enables wireless security.

`no security`

Disables wireless security.

security mode

Supported on: Wi² AP

`security mode (wep | tkip | ccmp)`

Set the security mode.

security psk

Supported on: Wi² AP

`security psk <secret>`

Sets the PSK secret.

`no security psk`

Clears the PSK secret.

security wep

Supported on: Wi² AP

`security wep <key>`

Sets the WEP key.

`no security wep`

Deletes the WEP key.

speed

Supported on: Wi² AP

`speed (auto | 1 | 2 | 5.5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54)`

Sets the speed of the wireless link in Mbps.

interface vlan

Supported on: Wi² AP

`interface vlan <id>`

Switches to the specified VLAN interface or create a new VLAN interface with the specified Id.

`no interface vlan <number>`

Removes the specified VLAN interface.

Parameters

<*id*>	**VLAN ID. Range: 1 - 4094.**

accept forced links

Supported on: Wi² AP

`accept forced links`

May accept master orders for selection.

`no accept forced links`

ignore master orders for selection.

allowed downtime

Supported on: Wi² AP

`allowed downtime <number>`

Set the allowed downtime for a connection (or a link) to a peer.

dynamic local mesh

Supported on: Wi² AP

`dynamic local mesh`

Use dynamic local mesh.

`no dynamic local mesh`

Use static local mesh.

dynamic mode

Supported on: Wi² AP

`dynamic mode (master | alt-master | slave)`

Selects the dynamic operation mode.

initial discovery time

Supported on: Wi² AP

`initial discovery time <number>`

Slave: Set the group's initial discovery time in seconds.

mesh id

Supported on: Wi² AP

`mesh id <id>`

Set the local mesh group id.

minimum snr

Supported on: Wi² AP

`minimum snr <number>`

Slave: Set the group's minimum SNR.

preserve master link

Supported on: Wi² AP

`preserve master link`

Preserve master link across reboots.

`no preserve master link`

Do not preserve master link across reboots.

promiscuous mode

Supported on: Wi² AP

`promiscuous mode`

Slave: Accept any group.

`no promiscuous mode`

Slave: Use only the slave's group.

promiscuous mode startup delay

Supported on: Wi² AP

`promiscuous mode startup delay <number>`

Set delay in seconds before promiscuous mode starts (if enabled).

snr cost per hop

Supported on: Wi² AP

`snr cost per hop <number>`

Slave: Set the group's SNR cost per hop.

2.11 RADIUS Context

Context path: View > Enable > Config > RADIUS

This context provides commands for configuring RADIUS profiles.

end

Supported on: Wi² AP

`end`

Switches to parent context.

radius-server accounting port

Supported on: Wi² AP

`radius-server accounting port <number>`

Specifies the port to use for RADIUS accounting.

Parameters

<number>	**Accounting port number. Range: 1 - 65535.**

radius-server alternate hosts

Supported on: Wi² AP

`radius-server alternate hosts`

Try last answering RADIUS host first.

`no radius-server alternate hosts`

Try primary RADIUS host first.

radius-server authentication method

Supported on: Wi² AP

`radius-server authentication method (mschap | chap | mschapv2 | pap | eap-md5)`

Sets the authentication method to use when communicating with the RADIUS server.

For 802.1x users, the authentication method is always determined by the 802.1x client software and is not controlled by this setting.

If traffic between the Wi² AP and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2, if supported by your RADIUS Server. (PAP, MSCHAP V1 and CHAP are less secure protocols.)

radius-server authentication port

Supported on: Wi² AP

`radius-server authentication port <number>`

Specifies the port to use for RADIUS authentication. By default, RADIUS servers use port 1812.

Parameters

<number>	**Authentication port number. Range: 1 - 65535**

radius-server deadtime

Supported on: Wi² AP

`radius-server deadtime <seconds>`

Sets the retry interval for access and accounting requests that time-out.

If no reply is received within this interval, the Wi² AP switches between the primary and secondary RADIUS servers (if defined). If a reply is received after the interval expires, it is ignored.

Parameters

<seconds>	**Retry interval. Range: 2 - 60 seconds.**

radius-server host

Supported on: Wi² AP

`radius-server host <primary>[<secondary>]`

Sets the addresses of the primary and secondary RADIUS servers.

Parameters

<primary>	**IP address of the primary RADIUS server.**
<secondary>	**IP address of the secondary RADIUS server.**

radius-server key 2

Supported on: Wi² AP

`radius-server key <primary>[<secondary>]`

Enter primary and secondary secrets.

Parameters

<primary>	**Shared secret for the primary RADIUS server.**
<secondary>	**Shared secret for the secondary RADIUS server.**

radius-server message-authenticator

Supported on: Wi² AP

`radius-server message-authenticator`

Include the message authenticator attribute in RADIUS packets.

`no radius-server message-authenticator`

Do not include the message authenticator attribute in RADIUS packets.

radius-server name

Supported on: Wi² AP

`radius-server name <name>`

Changes the name of the RADIUS profile.

radius-server nasid

Supported on: Wi² AP

`radius-server nasid <id>`

Sets the network access server ID you want to use for the Wi² AP.

By default, the serial number of the Wi² AP is used. The Wi² AP includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

radius-server timeout

Supported on: Wi² AP

`radius-server timeout`

Activates RADIUS timeout.

`no radius-server timeout`

Disables RADIUS timeout.

radius-server timeout

Supported on: Wi² AP

`radius-server timeout <number>`

Sets the total timeout for RADIUS requests.

`no radius-server timeout`

Disables RADIUS timeout.

2.12 IP_QOS Context

Context path: View > Enable > Config > IP_QOS

This context provides commands for configuring IP QoS profiles.

end

Supported on: Wi² AP

`end`

Returns to a previous context.

end-port

Supported on: Wi² AP

`end-port <number>`

Specifies the end port to use for this IP QoS profile.

Parameters

<number>	**End port number. Range: 0 - 65535**

priority

Supported on: Wi² AP

`priority <low | medium | high | very-high>`

Sets the priority for this IP QoS profile.

Parameters

<priority>	**Available priorities are: low, medium, high and very-high.**

profile name

Supported on: Wi² AP

`profile name <name>`

Changes the name of the IP QoS profile.

protocol

Supported on: Wi² AP

`protocol <number>`

Specifies the protocol ID use for this IP QoS profile.

Parameters

<number>	**Protocol number. Range: 0 - 255.**

start-port

Supported on: Wi² AP

`start-port <number>`

Specifies the start port to use for this IP QoS profile.

Parameters

<number>	**Start port number. Range: 0 - 65535**

2.13 GRE Interface Context

Context path: View > Enable > Config > GRE interface

Details of the GRE interface.

end force

Supported on: Wi² AP

`end [force]`

Quits the GRE context.

gre name

Supported on: Wi² AP

`gre name <name>`

Renames the current GRE interface.

ip address

Supported on: Wi² AP

`ip address <ip address>/<mask>`

Set the local tunnel IP address and mask.

peer ip address

Supported on: Wi² AP

`peer ip address <ip address>`

Sets the GRE peer IP address.

remote ip address

Supported on: Wi² AP

`remote ip address <ip address>`

Sets the remote tunnel IP address.

2.14 Syslog Destination Context

Context path: View > Enable > Config > Syslog destination

This context provides commands for configuring Syslog destinations.

active

Supported on: Wi² AP

`active`

Enables logging to the current destination.

`no active`

Disables logging to the current destination.

logging facility

Supported on: Wi² AP

`logging facility (local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7)`

Sets the facility that is used when logging messages to a syslog server.

Parameters

<facility>	**Available facilities are: local0 - local7.**

logging host

Supported on: Wi² AP

`logging host (tcp | udp) <addr> [<number>]`

Sets the remote address, the connection protocol and port of current syslog remote destination.

logging prefix

Supported on: Wi² AP

`logging prefix <string>`

Sets the prefix that will be prepended to all syslog messages.

`no logging prefix`

Removes the prefix that is prepended to all syslog messages.

name

Supported on: Wi² AP

`name <name>`

Renames the current syslog destination.

end

Supported on: Wi² AP

```
end
```

Switches to parent context.

level

Supported on: Wi² AP

```
level
```

Enables filtering of the log file by severity level.

```
no level
```

Disables filtering of the log file by severity level.

level

Supported on: Wi² AP

```
level (lower | higher) (debug | info | notice | warning | error | critical | alert | emergency)
```

Defines the severity of messages that will be logged.

```
no level
```

Disables filtering of the log file by severity level.

Parameters

`debug`	**Debug-level messages.**
`info`	**Informational messages.**
`notice`	**Normal, but significant condition.**
`warning`	**Warning conditions.**
`error`	**Error conditions.**
`critical`	**Critical conditions.**
`alert`	**Action must be taken immediately.**
`emergency`	**System is unusable.**

matches

Supported on: Wi² AP

```
matches (any | all) filters
```

All three log file filters (message, process, and level) are combined to filter the log according to this setting.

message

Supported on: Wi² AP

```
message
```

Enables filtering of the log file message field.

`no message`

Disables filtering of the log file message field.

message

Supported on: Wi² AP

`message (matches | notmatches) <regex>`

Use this filter to include log messages. Use a regular expression to define the match criteria for the log file message field.

process

Supported on: Wi² AP

`process`

Enables filtering of the log file by process name.

`no process`

Disables filtering of the log file by process name.

process

Supported on: Wi² AP

`process (matches | notmatches) <string>`

Use this filter to include log messages according to their process name.